CHAPTER

17

NETWORKING FUNDAMENTALS AND THE INTERNET

In this chapter, you will learn:

- About the typical hardware components of a network
- How several popular network technologies manage data traffic
- How data is transmitted over several interconnected networks
- How communications layers and their protocols are used on a network
- About many of the popular applications used on a network
- How to connect to a network using a modem and a phone line
- About the Internet and how to support PCs connected to the Internet

More and more PC users are connecting to the Internet from a home PC or connecting to a network at their places of business. So, you have to understand networking if you plan to manage and maintain a personal computer. This chapter first looks at the fundamentals of the hardware and software that make up networks, and then turns to the largest network of all, the Internet, and explains how to support a PC that interfaces with the Internet.

An Overview of Networking

Networking is a means of connecting computers together so that they can share data, such as files and programs, and resources, such as printers and modems. As with all other computer-related subjects, networking can be separated into two categories: network hardware and network software. This chapter addresses both the hardware and software used by networks, with the focus on how networking relates to personal computers.

Network architecture is the overall design of the network, including the physical components, network technologies, interfacing software and their protocols needed to establish reliable communication among each computer or workstation, which is called a network station, a **node**, or a **host**. Data is sent over a network as bits and bytes that have been translated into electronic signals. Before being transmitted, data is first divided into segments, each of which has a header and trailer attached. The headers and trailers are called a **frame** and the entire unit is called a **packet**. Each data packet is sent as an independent unit over the network. At the receiving end, the header and trailer information is removed, and the data within the several packets is reassembled into contiguous data.

You can think of this process of sending data over a network as similar to that of shipping a computer to a destination. The computer is first disassembled and packed into several boxes. When the boxes all arrive, the components are unpacked and reassembled into a complete computer. Think of the computer as data, its various components as data segments, and the shipping boxes with address labels as the headers and trailers. The units (the combination of shipping boxes, labels, and computer components) are the data packets. While in transit, the computer (or data) cannot function as a computer because it has been temporarily disassembled. But once it arrives at its destination, the packing is removed, and the computer is reassembled and made ready for use.

Just as an address is information written on a shipping box, a **header** is information sent in front of data to identify for receiving protocols the data destination and the protocols that the packet is using. A **trailer** follows the data and contains information used by some protocols for error checking. For example, in PCs, the firmware on the network card breaks the data into segments and encloses each segment between headers and trailers, thus creating individual packets. In addition, on the receiving end, the firmware on the network card reassembles the segments back into contiguous data. In the computer shipping analogy, think of the network card in the sending PC as the packing and shipping department, and the network card in the receiving PC as the person who receives the boxes, unpacks them, and assembles the computer system.

Remember that there are two approaches to managing a network: a peer-to-peer network where each individual workstation manages its own security and resources, and a client-server network that is managed by a server. As you learned in Chapter 13, Windows NT calls these two types of networks workgroups and domains, respectively.

The OSI Layer Network Model

In the 1970s, when manufacturers were beginning to build networking software, firmware, and hardware to connect computers, each manufacturer developed its own standards of communication within its proprietary network design. In the early 1980s, manufacturers began to make attempts to standardize networking so that networks from different manufacturers could communicate. Two bodies that were leaders in this standardization are the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE). For example, one major effort of the IEEE was to standardize **Token Ring** and **Ethernet** protocols, which are both considered industry standards for network cards and other network hardware devices that together make up the physical devices that form a network. Ethernet and Token Ring networks are discussed later in the chapter.

Proposed new standards are presented to the industry in the form of a **Request for Comment** (**RFC**), which is assigned a number to identify it. The RFC is publicized and discussed at large, and either adopted or rejected by the industry. You can search for and view the many RFCs that pertain to networking and the Internet at this web site: *www.rfc-editor.org*.

In an overall effort to identify and standardize all the levels of communication needed in networking, ISO developed a networking model called the **Open Systems Interconnect (OSI)** reference model, which is illustrated in Figure 17-1. This model breaks down the communication needed for one user or application to communicate with another over a network into seven logical levels. This model can be understood in much the same way as the model for communications over phone lines shown in Chapter 16, Figure 16-3, except that the OSI model covers strictly software and firmware, not hardware. Communication between adjacent layers is considered direct, but communication between matching layers is considered logical or virtual.

When studying the OSI model, remember that not all networks have a separate software or firmware layer that matches each of the seven layers. Realistically, no network in use today perfectly follows the model. However, the model does serve the networking industry as a reference point for discussing different levels or layers in a network. For example, firmware on a network card operates in the physical layer and the data-link layer in the model. From Figure 17-1, we see that the data-link layer is responsible for disassembling data into segments to be assigned to separate packets and later reassembling packets into contiguous data. The physical layer is responsible for passing packets to and receiving packets from the network media or cabling.

For our discussions, it would be unproductive to try to distinguish which portion of firmware on a Token Ring or Ethernet network interface card (NIC) is the data-link layer, and which portion is the physical layer. However, it is useful to talk about Token Ring and Ethernet covering these two layers and then to look for other software or firmware on the network that is managing the layers higher up in the model. For example, once you know that an Ethernet network handles the bottom two layers of data transmission, you can ask the question, "What software on the network determines the best possible route to send a packet so it can arrive at its destination?" This question is addressed by the network layer. The answer will not be found on the firmware of the Ethernet card, because Ethernet does not

encompass the network layer of the OSI model. By referring to the OSI model, manufacturers have a structure from which to work as they develop and enhance new networking software, protocols, and designs.

Without getting too deeply into the details of the OSI model, the following provides an overview of the role each layer plays in a network, starting at the top.

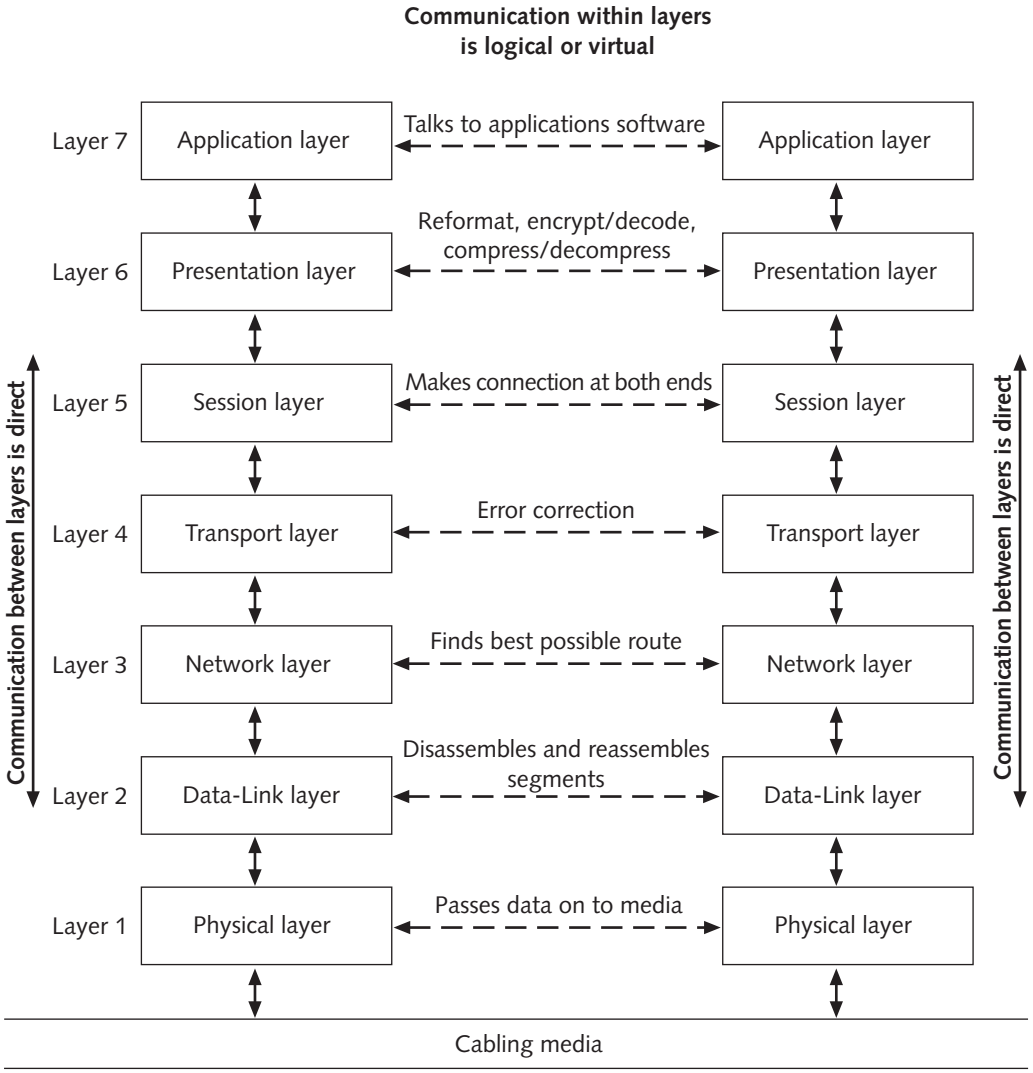


Figure 17-1 The OSI reference model identifies seven layers of network communication within software and firmware

Application Layer

The **application layer** of the OSI model is responsible for interfacing with the applications software using the network. For example, suppose you are using a word processor such as Microsoft Word. Word can open a document file that is stored on your hard drive (drive C), and it can just as easily open a document file stored on a file server connected to the LAN. The file server is known to the word processor as just another drive, such as drive F. You can open C:\Data\Myfile.doc or F:\Data\Myotherfile.doc. When the word processor attempts to open the file on drive F (which is the file server), it communicates the request to the application layer of the network software. The communication over the network is transparent to the application from that point forward. The file is retrieved over the network and presented to the word processor by the OSI application layer. An example of software that handles the application layer is NFS for Chameleon by NetManage (NFS stands for Network File Service).

Presentation Layer

The **presentation layer** receives requests for files from the application layer and presents the requests to the session layer (described below). Any reformatting, compressing, or encryption of data is performed by the presentation layer in order for the application layer and the session layer to communicate, for the data to be sent faster, or to secure the data.

Session Layer

The **session layer** is responsible for establishing and maintaining a session between two networked stations or nodes. A session over a network works somewhat like a telephone call over phone lines. The caller makes a call; someone answers on the other end. After both parties know that communication is established, conversation goes in both directions until either the caller or receiver ends the phone call. The session layer performs similar duties. An attempt is made to establish a session between two nodes on a network. Both nodes acknowledge the session, and the session is usually assigned an identifying number. Either node can disconnect a session when communication in both directions is completed. Sometimes a session between two nodes on a network is called a **socket**. When a session is established, a socket is opened. A disconnected session is called a closed socket.

Transport Layer

The **transport layer** is responsible for error checking and requests retransmission of data if errors are detected. The transport layer guarantees successful delivery of data.

Network Layer

The **network layer** is responsible for finding the best possible route by which to send frames over an internetwork (a network of networks). The two most common protocols that make up both the transport layer and the network layer are **TCP/IP** (**Transmission Control Protocol/Internet Protocol**) and **IPX/SPX** (**Internetwork Packet Exchange/Sequenced Packet Exchange**), which are both supported by Windows NT,

Windows 2000, and Windows 9x. For TCP/IP, which is used by the Internet, the TCP portion of the protocol is responsible for error checking, and therefore operates in the transport layer. The IP portion of the protocol makes up the network layer and is responsible for routing. IPX/SPX is used by NetWare by Novell, one of the most popular network operating systems for LANs. The IPX portion of the protocol is the network layer responsible for routing, and the SPX portion of the protocol manages error checking, making it the transport layer. These network protocols are further discussed later in the chapter.

Data-Link Layer

The **data-link layer** is responsible for receiving data packets from the network layer and splitting them up into segments of bits to be presented to the physical layer for transport. When data is received from the physical layer, the bits are reconstructed into packets to be presented to the network layer. Token Ring and Ethernet firmware on network cards are examples of code that handles both the data-link and physical layers of the OSI model.

Physical Layer

The OSI **physical layer** on a PC is controlled by the firmware on the network card. It includes the IEEE specifications for cabling types connected to the card and other media definitions. This layer controls how data is transmitted over the physical media. At this level, data is nothing but indistinguishable bits. Remember that data is packaged within frames before it is transmitted. This packaging of data has already occurred before this layer; the physical layer does not distinguish the frame header or trailer from the payload, or data, within the frame. The physical layer sees all of it as just bits that need to be passed on.

Data Frames

Remember that data is segmented and enclosed in frames before it is transmitted over a network as data packets. Each layer in the seven-layer model can add information to the beginning and ending of a data packet to be read by the counterpart layer on the receiving workstation. In practice, however, only the data link layer adds both a header and a trailer. The physical layer adds neither, and the other layers might or might not add a header. At its most complex stage, a packet may look like that in Figure 17-2, in which each layer that adds a header or trailer has added its identifying information to the packet.

Later, when the packet is presented to the counterpart layer on the receiving station, that layer interprets any information in the header and trailer intended for that layer. Then it strips off that header and trailer and passes the packet to the next higher layer in the model. For packets to transmit successfully, each layer of the OSI model must communicate using the same protocol as its counterpart layer on the remote computer.

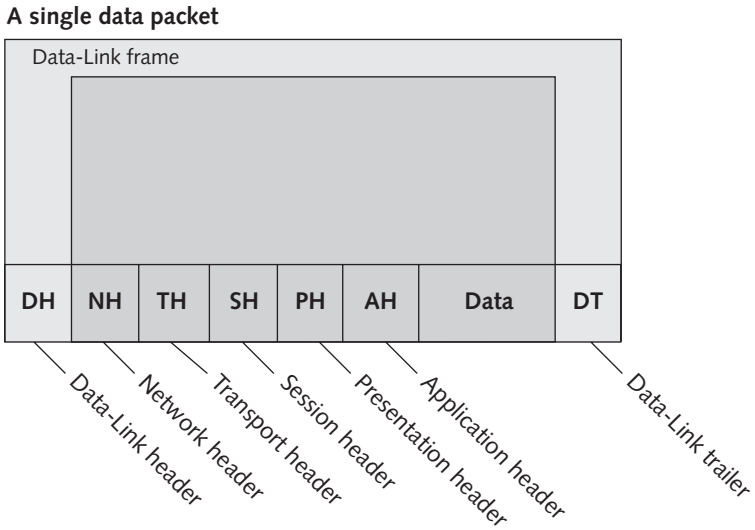


Figure 17-2 Any layer of the OSI model can add identifying information to a single data packet, either as a header or trailer, although, in practice, only the data-link layer uses both a header and a trailer and the physical layer uses neither

The rest of this chapter is generally organized around the OSI networking model, starting at the bottom. You will first learn about the bottom two layers—the physical and data-link layers—of the OSI model and also study the different hardware components (network cards, cables, and so forth) that these layers connect to. Then the chapter turns to the next two layers in Figure 17-1, the network and transport layers, and discusses the most popular protocol at these layers, TCP/IP, which is used by the Internet. Lastly, the chapter focuses on the session, presentation, and application layers, the layers we, as users, are most familiar with, including OS functionality, web browsers, e-mail software, and the like.

Network Technologies

The two bottom levels of the OSI model, the data-link layer and the physical layer are more directly connected to the physical hardware devices that form a network than other layers in the OSI model. Which device drivers and network card firmware operate at the data-link layer and physical layer is determined by the physical technologies used to create the network. These physical technologies and related network hardware devices are the subjects of this section.

The three most popular physical network technologies are Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). A relatively new type of network is Asynchronous Transfer Mode (ATM), which is a very fast network that works well over both short and long distances. An older type of network is Attached Resource Computer network (ARCnet), which is seldom seen today. Each type of technology is designed to solve certain network

problems, and each has its own advantages and disadvantages. Network technologies differ from each other in many ways. The coverage of some detailed differences is beyond the scope of this book. However, two basic differentiating characteristics—how computers are logically connected and how traffic is controlled on the network—are discussed here.

A network can be a LAN (local area network, typically a network in a single building or adjacent buildings, with nodes connected by cables) or a WAN (wide area network, covering a large geographical area, with nodes connected by methods other than cables, such as microwave signals). Several networks of either type can be tied together, which is called an **internetwork**.

Ethernet

Ethernet is the most popular network technology used today. Ethernet networks can be configured as either a bus topology or a star topology. **Topology** is the arrangement or shape used to physically connect devices on a network to one another. Figure 17-3 shows an example of a bus and a star topology. A **bus topology** connects each node in a line and does not include a centralized point of connection. Cables just go from one computer, to the next one, and the next. A **star topology** connects all nodes to a centralized **hub**. PCs on the LAN are like the points of a star around a central hub.

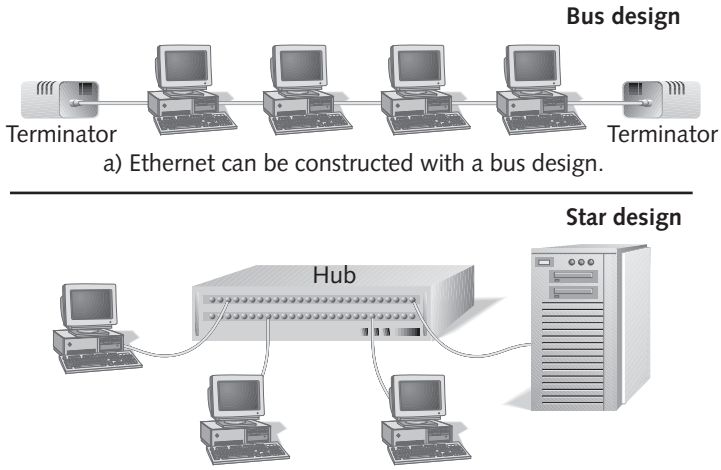


Figure 17-3 Ethernet is a simple and popular networking topology

The star arrangement is more popular because it is easier to wire and to maintain than is the bus arrangement. In a bus arrangement, the failure of one node affects all the other nodes. In a star arrangement, some hubs are called **intelligent hubs** because they can be remotely controlled from a console, using network software. Intelligent hubs can monitor a network and report errors or problems. With intelligent hubs, stations that are having problems can be remotely disabled from network access without affecting the rest of the network.

An Ethernet network is a passive network, meaning that the networked computers, rather than a dedicated network device, originate the signals that manage the network. (A dedicated network device is a device, such as a hub, used solely to support a network; other devices on the network, such as PCs, have functions other than networking.) Ethernet works much like an old telephone party line, where each computer is like a party line caller. When someone on a party line wanted to use a phone, he or she would pick up and listen. If there was a dial tone (carrier), then the person could make a call. If someone else was talking, the person would hang up and try again later. If two people attempted to make a call at the same time, both calls would fail. They would each need to hang up and begin again. The first one back on the line would be able to make a call.

A+CORE 6.1

Similarly, a computer that wants to send packets over Ethernet will first listen on the network for silence. If it hears nothing, it begins to transmit. As it transmits, it is also listening. If it hears something other than its own data being transmitted, it stops transmitting and sends out a signal that there has been a **collision**, which occurs when two computers attempt to send data at the same time. A collision can corrupt packets the computers recently sent. Each computer waits for a random amount of time and then tries to transmit again, first listening for silence. This type of network technology is called a **contention-based** system because each computer must contend for an opportunity to transmit on the network. Computers using Ethernet are said to gain access to the network using the **Carrier Sense Multiple Access with Collision Detection** (**CSMA/CD**) method. The name of the method suggests three characteristics of the way computers communicate on Ethernet: (1) a computer must sense that the network is free to handle its transmission before initiating a signal (carrier sense), (2) many computers use the same network (multiple access), and (3) each computer must detect and manage collisions (collision detection).

A+CORE 1.4

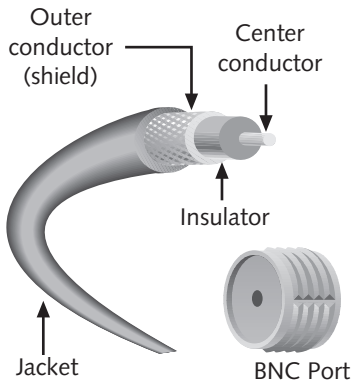
Ethernet can use any one of six cabling systems, which are described in Table 17-1. Figure 17-4 shows an example of each of these cables. The two most popular Ethernet cabling systems are 10BaseT and 10Base2 (Thinnet).

A+CORE 1.4, 6.1

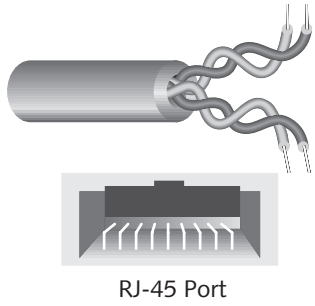
Table 17-1 Cabling systems used by Ethernet

Cable System	Cable and Connectors	Description
10Base5 (Thicknet) Speed = 10 Mbps	Thick coaxial cable uses an AUI 15-pin D-shaped connector.	Coaxial cable is made of two conductors: a center wire and a metallic braid that surrounds the center wire. Foam insulation separates the two. The maximum segment length of Thicknet is 500 meters.
10Base2 (Thinnet) Speed = 10 Mbps	Thin coaxial cable uses a **BNC connector** (T-connector).	A less expensive, smaller coaxial cable than Thicknet, with a maximum segment length of 185 meters. Thinnet and Thicknet are sometimes used on the same network.
10BaseT (Twisted pair) Speed = 10 Mbps	Unshielded twisted-pair (UTP) cable uses an **RJ-45 connector**.	Two pairs of wire, each insulated from the other and twisted together inside a plastic casing to lessen crosstalk and outside interference. (**Crosstalk** is the interference that each wire produces in the other.) There are several grades of UTP. (A lower grade of UTP not suitable for 10BaseT is often used for telephone wire.)
100BaseT (Fast Ethernet) Speed = 100 Mbps	Unshielded twisted pair (UTP) or Shielded twisted pair (STP) cable with RJ-45 connector. Category 5 (Cat-5) UTP cable is most common.	STP costs more than UTP and thin coaxial cable, but less than thick coaxial cable and fiber-optic cable. STP is rigid and thick and has a shielding around the twisted wires to protect them from outside interference. (Sometimes a very high grade of UTP can also be used for Fast Ethernet for local connections.)
10BaseFL and 100BaseFX (Fiber-optic) Speeds = 10 Mbps or 100 Mbps	Optical fiber (fiber-optic cable) uses an ST or SC fiber-optic connector.	These cables use light rather than electricity to transmit signals. A glass or plastic fiber in the center of the cable, about the same diameter as a human hair, transmits the light.

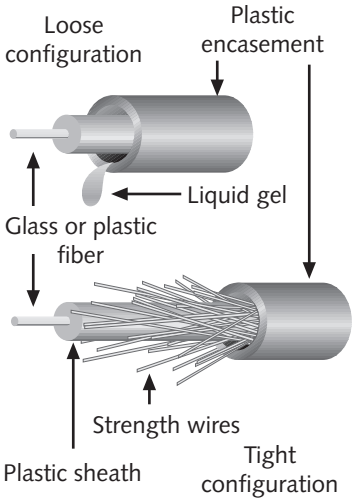
A+CORE 1.4, 6.1



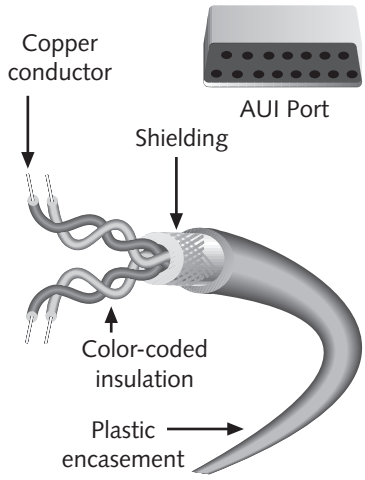
a) Coaxial cable



b) Unshielded twisted pair (UTP)



c) Fiber-optic cables with tight and loose sheaths



d) Shielded twisted pair (STP)

Figure 17-4 Networking cables

17

The "10" in 10BaseT comes from the speed of transmission (10 Mbps). The "Base" comes from **baseband**. Ethernet is a baseband network, which carries data over wire a single message at a time in digital form. Contrast baseband to a **broadband** network such as ATM or cable modem that carries multiple messages over wire, each message traveling on its own frequency in analog form. The "T" in 10BaseT stands for twisted-pair cabling.

A 10BaseT network uses a star topology (see Figure 17-5) with each PC on the network connected to a hub, although it is possible to connect two PCs together for a simple 10BaseT network without a hub. 10BaseT networks use RJ-45 connectors, which look like large phone jack connectors.

A+CORE 1.4, 6.1

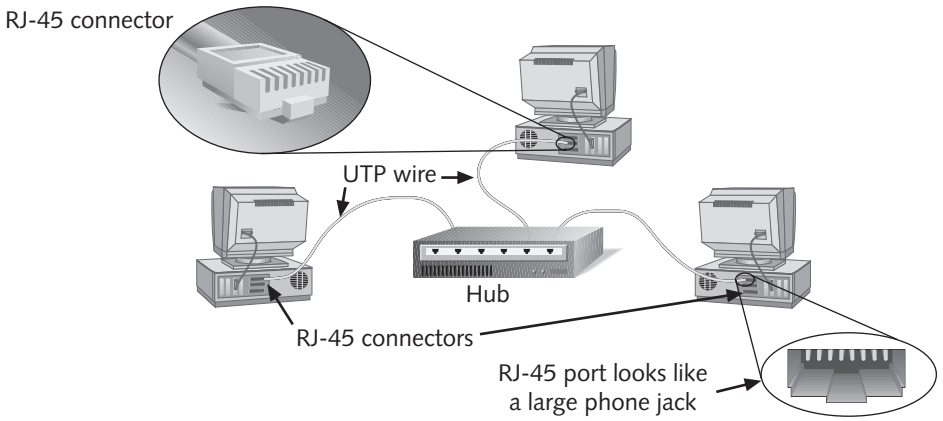


Figure 17-5 The popular Ethernet 10BaseT network uses unshielded twisted-pair (UTP) wire, RJ-45 connectors, and a star topology commonly using a hub

Thinnet (10Base2) networks use coaxial cables and BNC connectors, which are sometimes shaped like Ts (see Figure 17-6). Thinnet networks use a bus topology with terminators at each end of the bus that twist into the T-connectors at the back of the two end PCs. The BNC port on the network card looks like a cable TV connection.

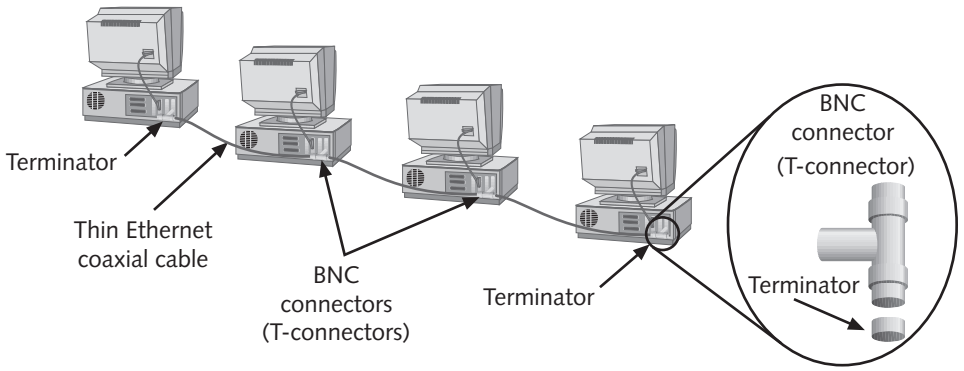
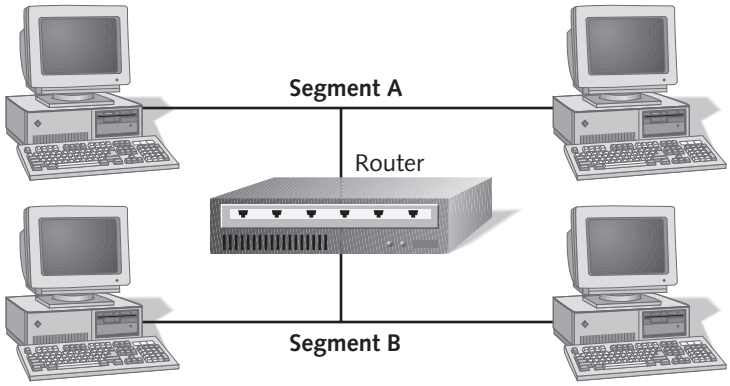


Figure 17-6 An Ethernet 10Base2 (Thinnet) network uses coaxial cables and BNC connectors, with terminators at each end of the network bus

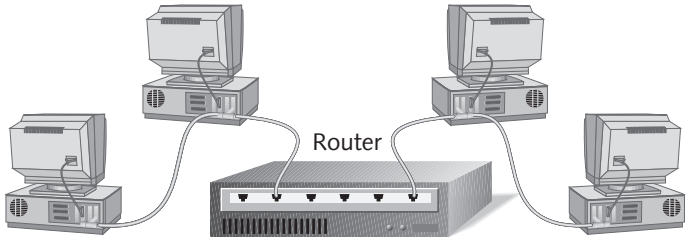
Because signals transmitted over long distances on a network can weaken, devices are added to strengthen the signals. For example, for a 10BaseT Ethernet cable, if the cable exceeds 100 meters (328 feet), signal strengthening is required. A **repeater** is a device that strengthens signals on a network. There are two kinds of repeaters. An **amplifying repeater** simply amplifies the incoming signal, noise and all. A **signal-regenerating repeater** "reads" the signal and then creates an exact duplicate of the original signal before sending it on. Baseband networks such as Ethernet use a signal-regenerating repeater and broadband networks such as ATM use amplifier repeaters.

A+CORE 1.4, 6.1

Each of the cable systems listed in the table can support only a limited number of nodes. As the number of nodes increases, performance speed and reliability can drop for the overall network. One method used to prevent this kind of congestion is **segmentation**. Segmentation splits a large Ethernet into smaller Ethernet segments. Each segment contains two or more computers and is connected to the other segments by a **router**, **switch, gateway**, or **bridge**. The differences among these devices are discussed later in the chapter. Stations on a single segment only need to contend with other stations on the same segment to send their packets. For example, in Figure 17-7, a router connects two Ethernet segments. The router transfers packets to another segment only when it knows that the packet is addressed to a station outside its segment. All other network traffic is contained within the segment. Don't let the two T shapes in Figure 17-7a confuse you. The Ts logically exist, but do not physically exist. If you were to wire these four PCs and one router together, the physical diagram could look like Figure 17-7b. You will learn more about routers later in the chapter.



a) Logically, a bridge connects two Ethernet segments.



b) Physically, the PCs and bridge can be cabled together in this manner.

Figure 17-7 A bridge connects two Ethernet segments

Token Ring

Token Ring networking, which was developed by IBM, is more complex and expensive, but more robust and reliable, than Ethernet. Because of its complexity, it is more difficult to maintain than Ethernet.

Connecting Components on a Token Ring

Logically, Token Ring networks are rings. However, physically, stations are connected to the network in a star formation. Each station connects to a centralized device called a **controlled-access unit** (**CAU**), a **multistation access unit** (**MSAU** or sometimes just **MAU**), or a smart multistation access unit (SMAU). Figure 17-8 shows one Token Ring configuration using two IBM 8228 MSAUs. Each MSAU shown in the figure can connect eight workstations to the network, and, with this type of MSAU, there can be as many as 33 MSAUs on one Token Ring network. One MSAU can connect to another by a cable called a patch cable. One end of each MSAU has a Ring In (data flows into the MSAU) or Ring Out (data flows out from the MSAU) connection. The main ring is composed of the MSAUs and the cables connecting them, which are together referred to as the main ring cable. (The cable connecting the last MSAU Ring Out to the first MSAU Ring In is not considered a patch cable.) The main ring cable can be fiber-optic.

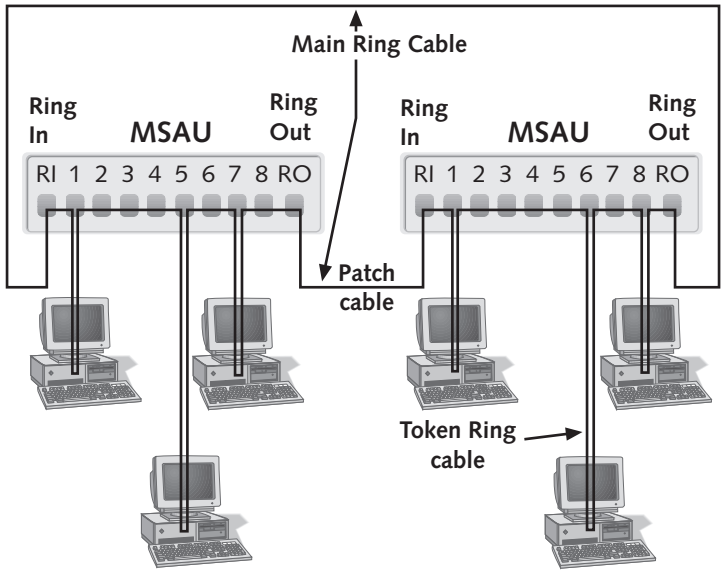


Figure 17-8 A Token Ring network uses one or more centralized hubs called multistation access units

The entire token ring is made up of not only the main ring, but also the cabling to each PC on the token ring. Each workstation contains a Token Ring LAN card with a 9-pin connector for the Token Ring cable, which connects each workstation to an MSAU. Each Token Ring network card has a unique address, which is assigned to it during manufacturing and encoded on the card's firmware. Token Ring cables can be either UTP or STP cables that have two twisted pairs, or four total wires in the cable.

Looking at Figure 17-8, you can see why a Token Ring network is said to be a physical star but a logical ring. All workstations connect to a centralized MSAU (in this case, two MSAUs), but you can also follow the ring path around the entire network. The ring path in

the figure goes from the first MSAU to each PC and back again, across the patch cable to the next MSAU, from this MSAU to each PC connected to it and back again, and finally, around the main ring cable back to the first MSAU.

Communication on a Token Ring

Communication and traffic on a Token Ring network are controlled by a **token**, which is a small frame with a special format that travels around the ring in only one direction. One station receives the token from the preceding station, called its **nearest active upstream neighbor** (**NAUN**), and passes it on to the next station on the ring, called its **nearest active downstream neighbor** (**NADN**). As one station passes the token to the next station, it can attach data in a frame to the token. The next station receives the token together with the data frame and reads this data frame. If the frame is intended for it, it changes 2 bits in the frame to indicate that the data has been read by the intended station. It then passes the token and the data frame on. When the token and frame are received by the station that sent the frame, it sees that the frame was successfully received and does not send the frame again. In this case, it releases the token by passing it on to the next PC, without a data frame attached. However, if the amount of data requires more than one frame, instead of releasing the token, the PC sends the next frame with the token. In either case, the token is passed on to the next PC, and data is never on the ring without the token preceding it.

Any PC receiving a token with no data frame attached is free to attach a data frame before passing on the token. The token is busy and not released to another PC until the sending PC has received word that the data was successfully received at its destination. In other words, the only PC that should remove a data frame from behind the token is the PC that attached it in the first place.

FDDI

Fiber Distributed Data Interface (**FDDI**, pronounced "fiddy") is a ring-based network, like Token Ring, but does not require a centralized hub, making it both a logical and physical ring. FDDI provides data transfer at 100 Mbps, which is much faster than Token Ring or regular Ethernet, and a little faster than Fast Ethernet, which also runs at about 100 Mbps. At one time, FDDI used only fiber-optic cabling, but now it can also run on UTP. FDDI is often used as a backbone network. A **backbone** is a network used to link several networks together. For example, several Token Ring and Ethernet networks can be connected using a single FDDI backbone.

FDDI uses a token-passing method to control traffic, but FDDI is more powerful and sophisticated than Token Ring. FDDI stations can pass more than one frame of data along the ring without waiting for the first frame to return. Once the frames are transmitted, the sending station can pass the FDDI token to the next station, so more than one station can have frames on the ring at the same time. With Token Ring, a data frame is only found traveling behind the token. With FDDI, data frames travel on the ring without the token. A PC keeps the token until it has sent out its data and then passes the token on. Possessing the token gives a PC the right to send data. A token is released (sent on) when the PC has finished transmitting.

Look at Figure 17-9, which shows a FDDI network with five stations. There are three frames of data currently on the ring, all sent from Station 1 to Station 5. Because Station 1 is finished sending its data, it has passed the FDDI token to Station 2. If Station 2 is ready to send data, it can do so now, although data from Station 1 is still on the ring. Another optional feature of FDDI is multiframe dialogs. **Multiframe dialogs** allow one station to send a **limited token** to another station. With this limited token, the second station can communicate only with the first station, not with other stations on the network. This "private conversation" allows for continuous communication between two stations without interference from other stations. At the same time, the main token can be active on the ring, allowing other frames to be passed among other stations.

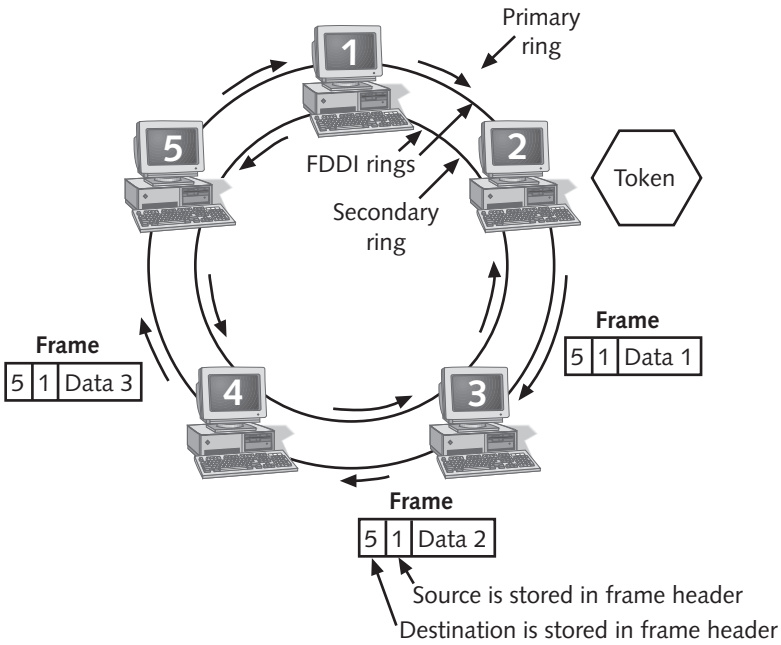


Figure 17-9 A FDDI network can have more than one frame of data on the rings. Shown here are three frames of data moving clockwise around the ring

One important strength of FDDI is its dual counter-rotating rings, as seen in Figure 17-9. Instead of a single ring like the one the Token Ring uses, FDDI has two rings linking each device on the network, a primary ring and secondary ring. Data normally travels on the primary ring. However, if a break occurs on the FDDI ring, any device can switch the data to the secondary ring, which causes the data to travel in the opposite direction back around the ring, as shown in Figure 17-10. When the data reaches the break coming from the other direction, a station switches the data back to the primary ring, and it continues in the opposite direction again. In this way, communication continues even with a break in one FDDI ring.

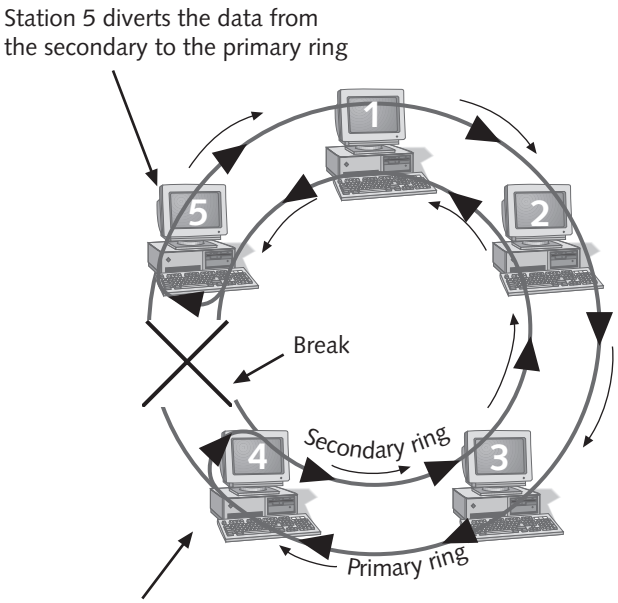


Figure 17-10 A break in the FDDI ring causes stations to divert data from one ring to another

Summary of Network Technologies

Table 17-2 shows a comparison and summary of the three network technologies discussed above.

Table 17-2 Comparing three popular network architectures

Item	Ethernet	Token Ring	FDDI
Logical topology or shape	Bus	Single ring	Dual ring
Physical topology or shape	Star or bus	Ring or star	Ring
Media	Twisted-pair, coaxial, or fiber-optic cable	Twisted-pair or fiber-optic cable	Primarily fiber-optic cable
Standard bandwidth	10 Mbps or 100 Mbps	4 or 16 Mbps	100 Mbps to 200 Mbps
How token is released	Not applicable	After receive	After transmit

Table 17-2 Comparing three popular network architectures (continued)

Item	Ethernet	Token Ring	FDDI
Maximum number of nodes	500	260	1024
Advantages	Of the three networks, Ethernet is the least expensive, simplest, and most popular solution.	Token Ring operates more reliably under heavy traffic than does Ethernet, but can be difficult to troubleshoot.	FDDI is much faster than Token Ring and regular Ethernet and faster than 100BaseT (Fast Ethernet).

Networking Hardware

Almost all LANs and WANs today are designed using a Token Ring, Ethernet, FDDI, or possibly ATM technology. Besides network cards in the PCs and cabling connecting them, there are other devices needed to physically construct a network. It is beyond the scope of this book to cover all the many hardware components needed to make a LAN or WAN work, but this chapter introduces a few common components. Recall that, for a PC, the direct connection to a network is by way of a network interface card (NIC). Sometimes the logic normally contained on the NIC is on the system board, with a network port coming directly off the system board. This is a common practice for Compaq and Macintosh computers. Hubs are used to provide the centralized location for nodes to connect on a star network. Bridges, switches, routers, and gateways connect one network to another, each performing a slightly different function when connecting like and unlike networks.

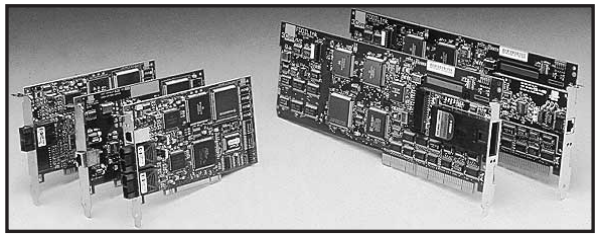
Network Interface Card (NIC)

A+CORE 6.1, 4.1

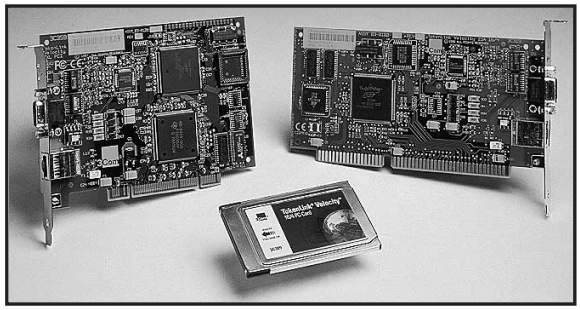
A **network interface card** (**NIC**) plugs into a system board and provides a port or ports on the back of the card for connection to a network. A NIC manages the communication and network protocol for the PC. A NIC is designed to support Ethernet, Token Ring, or FDDI network topologies, but not all three. However, it might be designed to handle more than one cabling system. See Figure 17-11 for some examples of network cards. The network card and the device drivers controlling the network card are the only components in the PC that are aware of the type of network being used. In other words, the type of network in use is transparent to the applications software using it.

A+CORE 6.1, 4.1

a. FDDI



b. Token Ring



c. Ethernet

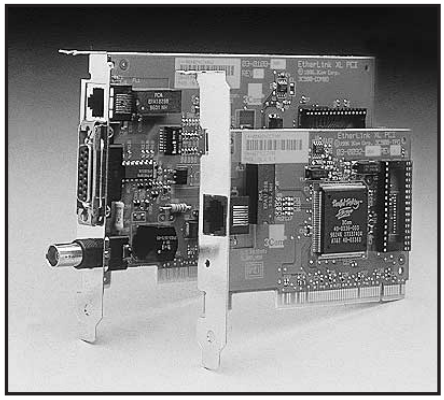


Figure 17-11 Three different types of network cards: (a) FDDI, (b) Token Ring, and (c) Ethernet

A network card sends and receives data to and from the system bus in parallel, and sends and receives data to and from the network in series (Figure 17-12). In addition, the network card is responsible for converting the data it is transmitting into a signal that is in a form appropriate to the network. For example, a fiber-optic FDDI card contains a laser diode that converts data to light pulses before transmission, and a twisted-pair Ethernet card that converts data from the 5-volt signal used on the computer to the voltage used by twisted-pair cables. The component on the card that is responsible for this signal conversion is called the **transceiver**. It is common for an Ethernet card to contain more than one transceiver, each with a different port on the back of the card, in order to accommodate different cabling media. This type of Ethernet card is called a **combo card** (see Figure 17-13).

A+CORE 6.1, 4.1

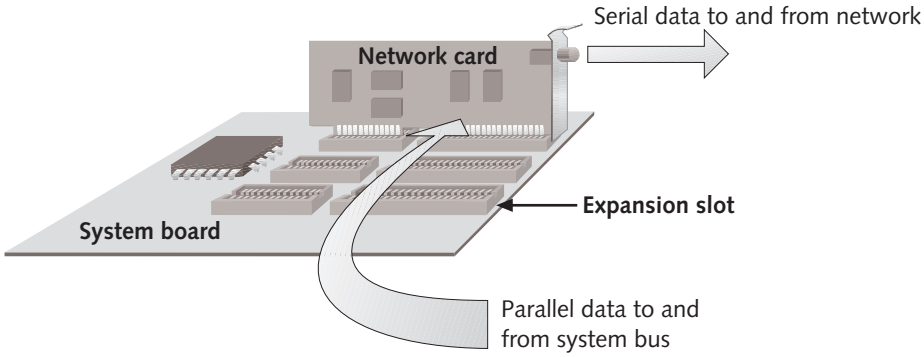


Figure 17-12 Network cards communicate with the network in serial, and with the computer in parallel

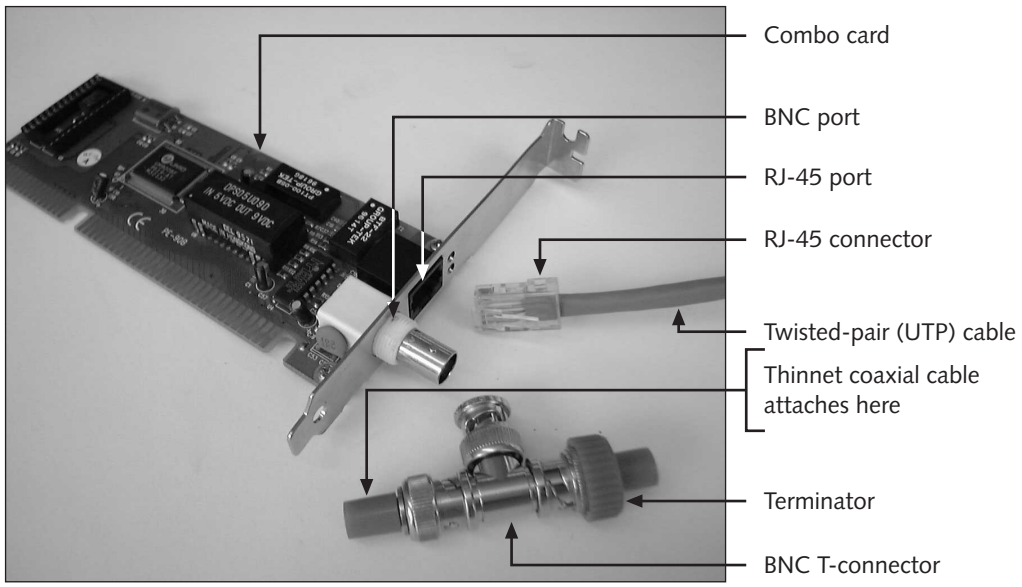


Figure 17-13 This Ethernet combo card can use either a BNC or RJ-45 connection, depending on the cabling system used

Different networks have different ways of identifying each node on the network. Ethernet and Token Ring cards have unique addresses hard-coded on the card by the manufacturer. Called **media access control** (**MAC**) addresses, **adapter addresses**, or, in the case of Ethernet, Ethernet addresses, these addresses are 6-byte hex addresses unique to each card. Part of the MAC address contains the manufacturer, and part of the address is unique to each card; therefore, no two adapters should have the same MAC address.

Network cards require an IRQ, an I/O address, and, for DOS and Windows 9x real mode, upper memory addresses. If the network card is on the PCI bus, then the PCI bus controller manages the IRQ and I/O address requirements. (See Chapter 9 for more information about

A+CORE 6.1, 4.1

configuring PCI devices.) Network cards may be Plug and Play, or they can use jumpers or DIP switches on the card to determine which resources to request. When selecting a network card, three things are important:

- The type of network you are attaching to (for example, Ethernet, Token Ring, FDDI, or a proprietary network standard)
- The type of media you are using (for example, shielded twisted-pair, coaxial, or fiber-optic cable)
- The type of I/O bus you are attaching the card to (for example, PCI or ISA. When selecting the bus to use, recall that PCI is faster than ISA and is the preferred choice. FDDI is much too fast a network for an ISA bus; always use a PCI bus with FDDI cards.)

Bridges, Switches, Routers, and Gateways

Remember that when more than one network is connected, the networks form an internetwork. For instance, a large Ethernet network can be broken into smaller, more easily managed segments, and a device is needed to bridge them. When two networks use different methods of transmission, such as Ethernet and Token Ring, then a device is needed to translate between the two networks. When many networks are interconnected, a device is needed that can choose the best route over these networks.

To satisfy these requirements, bridges, switches, routers, and gateways are used to connect networks and network segments to each other. Two reasons to internetwork are: (1) to extend the geographical area beyond what a single LAN can support, such as to different floors in a building or to other buildings, and (2) to decrease the amount of traffic on a single LAN by dividing the LAN into more than one network.

Bridges and switches connect network segments and work at the lower two layers of the OSI model. When a bridge or switch receives signals from one network segment, it makes an intelligent decision as to whether to pass the signals on to the next segment, based on the destination MAC address. In this way, the bridge or switch limits network traffic across it to only traffic going from one network segment to another, thus making the network more efficient. Using a bridge or switch on a network can improve network performance if the device is strategically placed in the network so that most traffic remains contained on its own side of the device. An example of breaking up a network to improve performance is when you isolate a group of computers that shares the same printers or files. The heavy traffic of this group communicating within itself does not affect the rest of the network.

Routers also connect networks, but work at the Network and Transport layers of the OSI model. Routers can also make intelligent decisions about how to route packets to other networks. For example, large networks are often logically divided into many smaller separate networks, and each small network is identified by a logical network address. These smaller networks are sometimes called **subnetworks**, or **subnets**. Now each packet or frame, in addition to having a physical device address, also has a logical network or subnet address. A router can make decisions as to which neighboring network to send a packet to, based on its ultimate destination subnet address.

Routers can be computers with operating systems and special network software, or they can be other dedicated devices built by network manufacturers. Routers hold tables of network addresses, along with the best possible predetermined routes to these networks. These **router tables** can also contain the cost of sending data to a network. The cost can be expressed in one of two ways (hop count is the more common method):

- **Hop count**: The number of routers a packet must pass through in order to reach its destination
- **Tick count**: The time required for a packet to reach its destination. One tick equals 1/18 second.

The routing tables are modified every few minutes to reflect changes in the networks. When a router rebuilds its router table based on new information, the process is called **route discovery**.

A **gateway** connects networks that use different protocols and translates these protocols. For example, a gateway can convert e-mail messages written in a proprietary e-mail format on a corporate WAN to a format that can be sent over the Internet before leaving the WAN. The gateway translates the outgoing network traffic to the protocol needed by the destination network. Gateways can even function so that a computer on one network that uses one protocol can use data from an application stored on a computer on another network that uses a different protocol. The term gateway also is sometimes loosely used to describe any device that acts as the entry or exit point for a network.

Networking Software Overview

Each of the seven layers in the OSI model uses different methods of communicating to its counterpart layer. These methods are called **protocols**. From the preceding discussion, you can see why there are many different protocols simultaneously in use when a network is working. You have seen that the two lowest layers (the physical and data-link layers) are controlled by the firmware on the network cards. However, most of the layers of the OSI model are controlled by the OS managing the network. The best-known network operating systems in the PC world are the UNIX operating system, NetWare by Novell, Microsoft Windows NT and Windows 2000. In addition to the OS that is managing the network, applications software such as Web browsers and e-mail clients are working at the top layers of the model. This section first looks at an overview of all the network software components, and then looks in detail at several of the more popular products used at the topmost layers of the OSI model, the ones users are most accustomed to seeing and using.

A map showing how the components of a network relate to one another and to the OSI model is shown in Figure 17-14. The figure is not intended to be comprehensive. There are user and applications services other than the ones listed, and networks other than Ethernet, Token Ring, FDDI, and phone lines. However, this figure shows how real-life networks map to the OSI model, moving from the lowest level at the bottom of the figure to the highest level at the top.

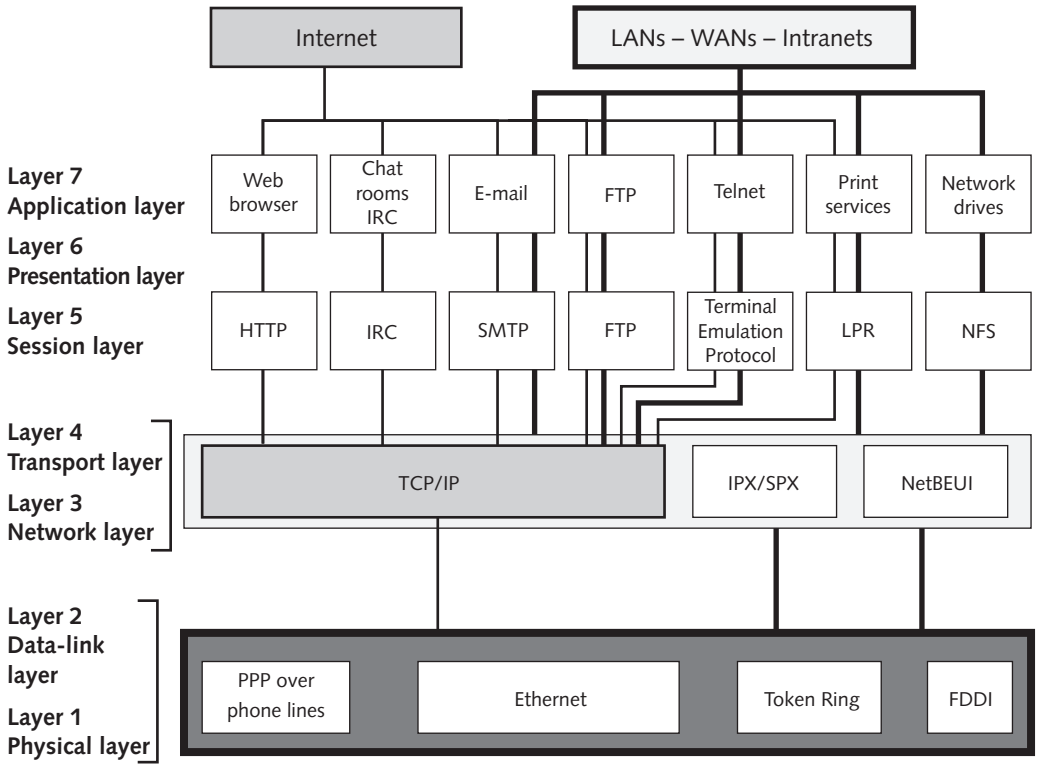


Figure 17-14 An overview of networking software showing the relationships among components

Network Protocol

A+ CORE 6.1, OS 4.1

The three network technologies shown in the bottom layer (physical and data-link layers) of Figure 17-14 have already been discussed: Ethernet, Token Ring, and FDDI. Also shown at the bottom layer is **PPP** (**Point-to-Point Protocol**) over phone lines, which is a protocol PCs with modems use to connect to a network. The Point-to-Point Protocol is the most popular protocol for managing network transmission from one modem to another. The next level up in the figure shows the network and transport layers, showing TCP/IP as the protocol used by the Internet. It is also used on LANs, WANs, and intranets. (An **intranet** is a private TCP/IP network used by a large company.) The IPX/SPX protocol is used primarily on Novell LANs. Since TCP/IP is becoming the most popular protocol at this level, Novell also supports TCP/IP as an alternate protocol. Less significant, but shown in the figure, is the **NetBEUI** protocol (**NetBIOS Extended User Interface**, pronounced "net-boo-ee"), a proprietary Microsoft protocol used only by Windows-based OSs (such as Windows for Workgroups) and limited to LANs, since it does not support routing. Other proprietary protocols that can be used at this level are XNS, DECnet, Vines, and AppleTalk for Apple and Macintosh computers.

A+CORE 6.1, OS 4.1

The higher layers in the network model shown in Figure 17-14 also use protocols to communicate with their counterpart services on the receiving node of the network. For example, when you send e-mail across a network, the e-mail is sent using **SMTP** (**Simple Mail Transfer Protocol**), which operates on the session layer. Network drives use NFS protocol, and the World Wide Web on the Internet uses **HTTP** (**Hypertext Transfer Protocol**), both of which operate on the session layer as well. Transferring files across the Internet is most often done using **FTP** (**File Transfer Protocol**). E-mail, the World Wide Web, and FTP are all discussed later in the chapter.

Network Services

At the highest level of the OSI model are the application and presentation layers. Users access some of these components directly, and others are designed to be interfaces between the network and applications software. Some of the more popular network applications offered at this level are listed below:

- **Web browsers**: Provide primary access to the Internet
- **Chat rooms**: Provide online, interactive communication among several people on the Internet
- **E-mail**: Provides electronic mail (which consists of text files) across the Internet or other networks
- **FTP**: Provides a method of transferring files from one computer to another
- **Telnet**: Provides a console session from a computer to a remote computer. (For example, a user can sit at a PC and use Telnet to connect to a remote UNIX computer and display a window on the PC screen that looks and acts just like the UNIX OS console. Using this window, the user can issue UNIX commands to control the UNIX computer from the PC.)
- **Print services**: Refers to sharing printers across a network
- **Network drive**: Hard drive space on one computer on the network made available to another computer as a virtual or logical drive for the remote computer

Two Network Configurations

A+CORE 6.1

Using Figure 17-14 as an anchor point, recall from Chapter 13 that a network can be logically configured either as a peer-to-peer network or as a network using a dedicated server. Figure 17-15 shows an example of a peer-to-peer network. Users at each workstation can use shared printers and files on each others' computers. The services on a peer-to-peer network are often limited to FTP, print services, and network drives. Nodes on a peer-to-peer network can communicate with any other node on the network and access files and other resources on that node, subject to security limitations. Each node is responsible for the security of its own resources.

A+CORE 6.1

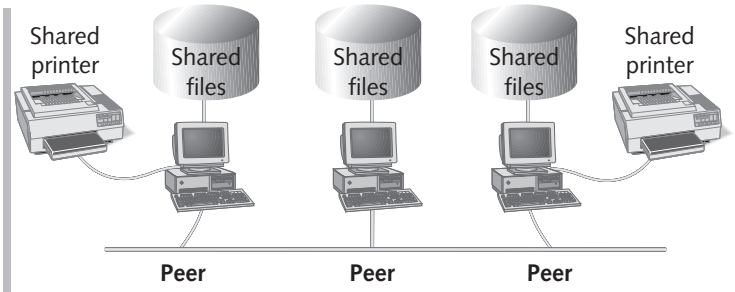


Figure 17-15 A peer-to-peer network allows all computers to share and use resources

A dedicated-server network, seen in Figure 17-16, has at least one computer, or server, on the network that serves the other computers on the network. If the server contains applications software together with data that is shared by other computers on the network (called clients, or workstations), then the network is called a client/server network. The application on the client that makes use of data stored on the server is called the **front end**. The application on the server that processes requests for data is called the **back end**.

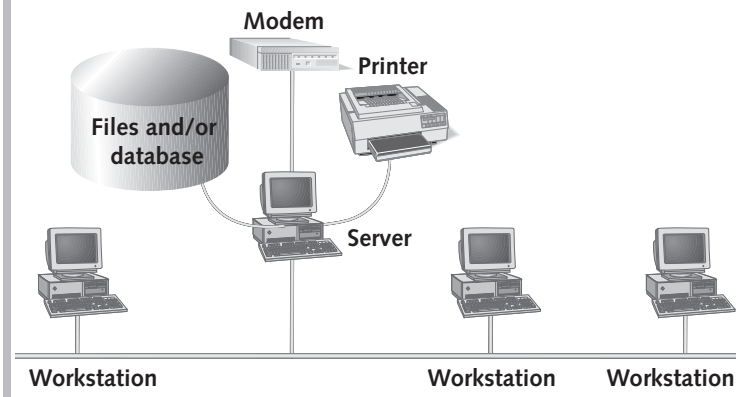


Figure 17-16 A dedicated-server network allows a server to make resources available to all workstations on the network

Dedicated-server networks can be used in one of two ways. If data is processed by the front end, and the server only holds the data, processing can be very slow because the client and server need to interact repeatedly. In a true client/server environment, the front end passes all information that is needed to process the data to the back end, and the back end does the processing. When the back end is finished, it can pass a positive response or a calculated answer back to the client. This last method requires less network traffic and is considered a better use of the network.

Looking back at Figure 17-14, all the programs listed at the application layer can operate on either a dedicated-server or peer-to-peer network. However, the World Wide Web, chat rooms, and e-mail always involve at least one dedicated server. A service that is not listed in the figure, but is used in a client/server environment, is the software necessary for an application on a

A+CORE 6.1 client to pass requests to a server, and for a server to respond with data. This type of software is called **middleware**. One popular example of middleware is Microsoft's Open Database Connectivity (ODBC) software. For instance, with ODBC, a front-end application on a client passes a request to update or query a database on the server. The ODBC back-end version of the software processes the request on the dedicated server and returns an answer to the client.

Networking with Windows 9x, Windows NT Workstation, and Windows 2000

This section discusses how Windows 9x, Windows NT, and Windows 2000 workstations can connect to a network, how to install a network card, and what you need to know when supporting PCs on a network. To connect to a network with Windows 9x or Windows NT Workstation, the networking portion of the OS must be enabled. Sometimes this process is more automatic than at other times. The proper hardware must be installed, along with the device drivers to use that hardware. The device drivers and firmware on modems and network cards generally operate at the physical and data-link layers of the network. The Transport and Network protocols must be installed and then bound to the modem or NIC.

At the transport and network layers, Windows 9x and Windows NT support three different transport and network protocols: TCP/IP, IPX/SPX, and NetBEUI. In addition, Windows 2000 supports AppleTalk. Each protocol can use three different methods for connecting to a network: (1) a network card (either Ethernet, Token Ring, or some other network technology), (2) direct cable connect (for example, using a serial or parallel port), and (3) dial-up networking (using a modem and phone lines). This section addresses these three methods of connecting to a network at this lowest level of networking.

Dial-Up Networking

A+CORE 6.1 When a Windows PC connects to a network using a modem and regular phone line, the process is called **dial-up networking** (**DUN**). In effect, the modem on the PC acts like a network card, providing the physical connection to the network and the firmware at the lowest level of communication. After the dial-up connection is made, the PC's applications software relates to the network as though it were directly connected to the network using a network card, but a network card is not needed. The modems and phone lines in between are transparent to the user, although transmission speeds with direct network connections are much faster than with dial-up connections. This section covers how to use Windows 9x, Windows NT, and Windows 2000 Dial-Up Networking utilities.

How Dial-Up Networking Works

Dial-up networking works by using PPP (Point-to-Point Protocol) to send packets of data over phone lines. The network protocol packages the data, making it ready for network traffic, and then PPP frames these packets. Figure 17-17a shows how this works. The data is presented to the network protocols, either TCP/IP, NetBEUI, or IPX/SPX, which add their frame

A+ CORE 6.1

information. Then the packet is presented to the line protocol, PPP, which serves as the data-link layer in the OSI model. The packet is encapsulated in the PPP header and trailer and then presented to the modem for delivery over phone lines to a modem on the receiving end.

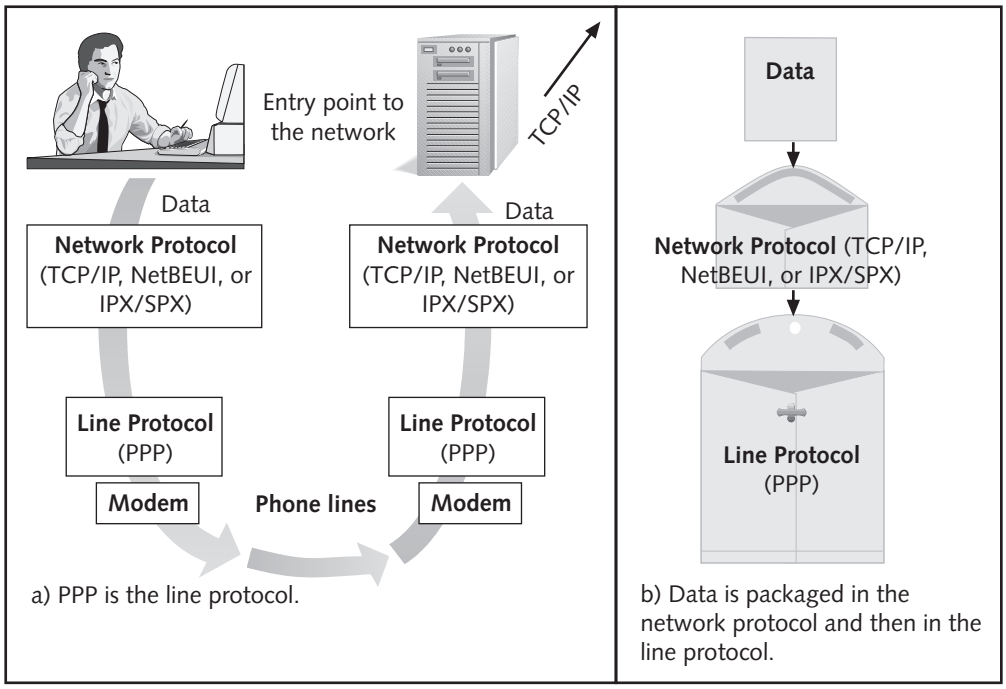


Figure 17-17 PPP allows a PC to connect to a network using a modem

The modem on the receiving end is connected to a PC or server. The receiving computer strips off the PPP header and trailer information and sends the packet on to the network still packaged in the TCP/IP protocols, or whatever other protocols the network is using. In Figure 17-17b, you can see how these two protocols act like envelopes. Data is put into a TCP/IP envelope for travel over the network. This envelope is put into a PPP envelope for travel over phone lines. When the phone line segment of the trip is completed, the PPP envelope is discarded.

PPP is sometimes called a bridging protocol or, more commonly, a **line protocol**. An earlier version of a line protocol is **Serial Line Internet Protocol** (**SLIP**), which is seldom used today.

17

A+ OS 4.1

Creating a Dial-Up Connection

To use Windows 9x or Windows NT Workstation to communicate to a network over phone lines; Dial-Up Networking must be installed as an OS component on your PC. (Windows 2000 Network and Dial-Up Connections is installed by default.) After installation, you then create an icon in the Dial-Up Networking group, and then use the icon to

A+ OS 4.1

make a connection. After the connection is made, any network service available on your network can be used if you have the software on your PC to support it. For example, a network drive is a useful method of passing files back and forth to and from a host computer or other computers on the network. However, experience says that FTP is a more reliable way to transmit files; the choice is yours. If you are using Windows 9x, follow these directions to create a connection using Dial-Up Networking. Windows 98 is used in this example, but Windows 95 works the same way:

1. If Dial-Up Networking is not installed, click **Start**, point to **Settings**, and click **Control Panel**. Double-click **Add/Remove Programs**.
2. In the Add/Remove Programs dialog box, select the **Windows Setup** tab.
3. Select **Communications** and click **Details**. The dialog box on the right in Figure 17-18 shows the components of the Communications group of Windows 98.

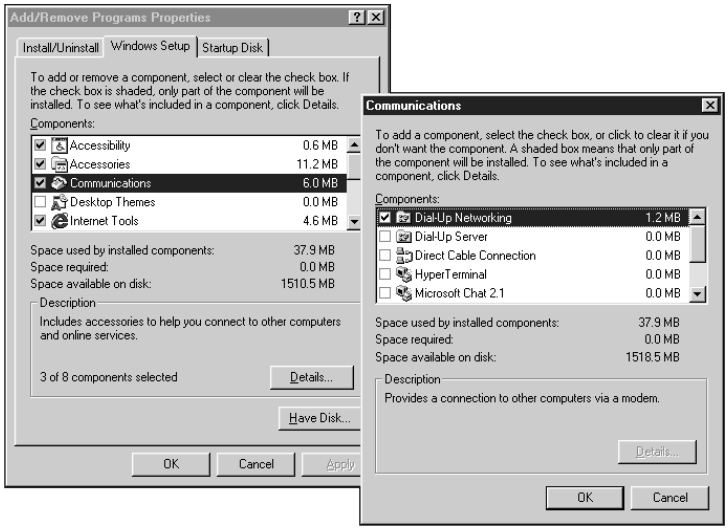


Figure 17-18 Use the Add/Remove Programs window to install Dial-Up Networking

4. If the Dial-Up Networking box is not checked, check it now, and click **OK** to install the component. You might be asked for the Windows 98 CD-ROM or disks.
5. After Dial-Up Networking is installed, click **Start**, point to **Programs**, **Accessories**, **Communications**, and then click **Dial-Up Networking**. The Dial-Up Networking dialog box appears, as in Figure 17-19.
6. Double-click **Make New Connection**. The Make New Connection dialog box appears, also shown in Figure 17-19.

A+ OS 4.1

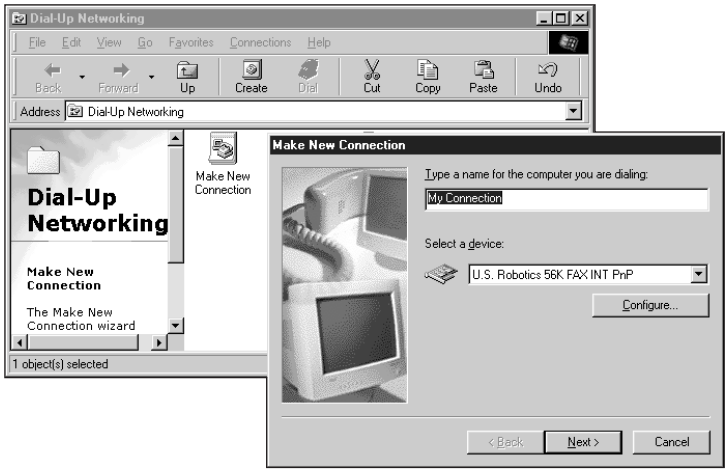


Figure 17-19 Creating a Dial-Up Networking Connection icon

7. Enter a description of the computer you will be dialing. If your modem is already installed, it appears in the modem list. If not, see Chapter 15 about installing modems.

8. If a logon is required, either before or after you dial into the network, you can request a logon window. Click **Configure** to see the Modem Properties dialog box shown in Figure 17-20.

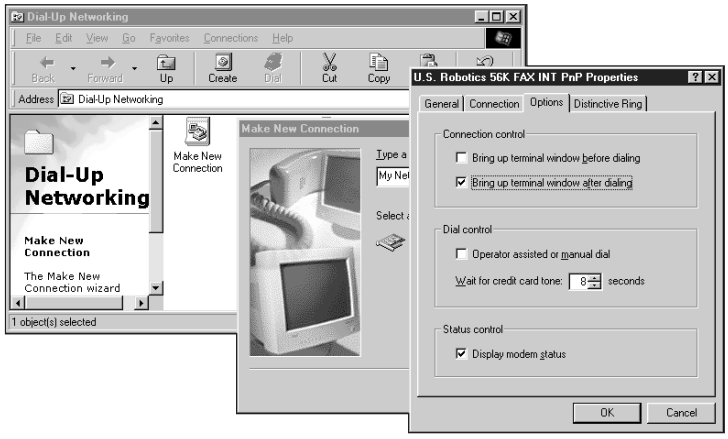


Figure 17-20 When setting up the logon interface, you can request that a terminal window be displayed before or after dialing

9. Click the **Options** tab, as in Figure 17-20. Select the option to display a terminal window before or after dialing, according to what the network needs. Click **OK** to return to the previous screen. Click **Next** to continue.

A+ OS 4.1

10. In the next dialog box, type the phone number to dial, and click **Next** to continue.
11. Click **Finish** to build the icon. The icon is displayed in the Dial-Up Networking window.
12. Dial-Up Networking uses default values for the properties of this icon. To view these values, right-click the icon and select **Properties** from the drop-down menu.
13. Click **Server Type**. Figure 17-21 shows the resulting dialog box. Notice that all three network protocols are selected, meaning that the connection supports whichever of the three the network is using. PPP for Windows 98, Windows NT Server, or the Internet is the selected Dial-Up Server. Click **Cancel** twice to return to the Dial-Up Networking window.

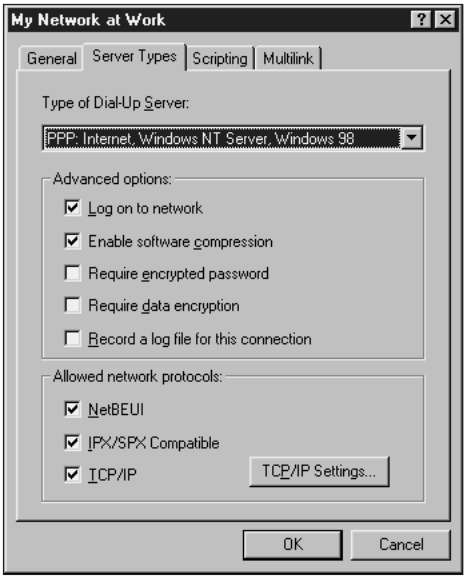


Figure 17-21 Properties of a Dial-Up Networking icon showing server types

14. To make a connection, double-click the icon you just created, and then click **Connect**. You should now hear the modem making the connection.

Dial-Up Adapter

When Windows 9x installs Dial-Up Networking, it also "installs" a Dial-Up Adapter. In terms of function, think of a Dial-Up Adapter as a virtual network card. It is a modem playing the role of a network card for Dial-Up Networking. After DUN is installed, open the Device Manager to see your "new" Dial-Up Adapter listed under Network adapters, as in Figure 17-22. You can also see it listed as an installed network component in the Network window of the Control Panel.

A+ OS 4.1

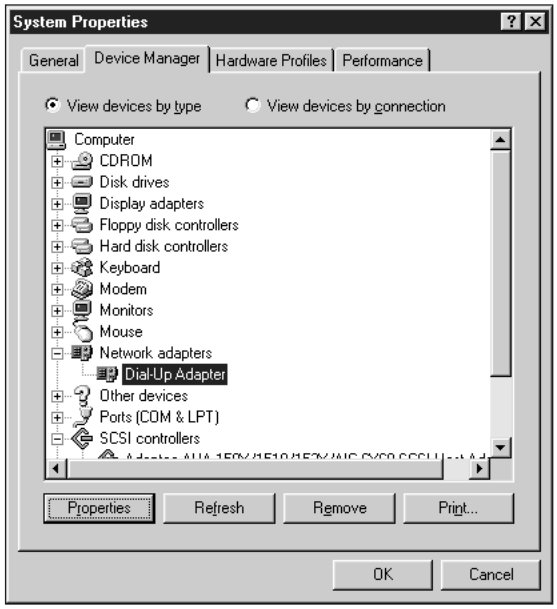


Figure 17-22 After Dial-Up Networking is installed, a new virtual network device, Dial-Up Adapter, is listed as an installed hardware device

After the Connection is Made

After you make a dial-up connection, you can do three things, depending on the type of computer or network you dialed. Each of the options listed below is discussed in more detail later in the chapter.

- If you are connected to an Internet service provider, you can use Internet programs installed on your PC such as e-mail or a web browser.
- If you are connected to another PC also running Windows 98, you can use files and printers on the other PC if the other PC has designated them for sharing. How to share resources between two computers is discussed under "Direct Cable Connect," coming up next.
- If you are connected to a LAN such as when you dial into a network at your workplace, from home or another remote location, you can gain access to resources on the LAN by using Network Neighborhood.

You can set up your PC to allow another computer to dial in. When using Windows 95, run the Microsoft Plus! utility. For Windows NT, install RAS, and for Windows 98, install Windows 98 Dial-Up Server. For Windows 2000, remote access is installed by default.

Direct Cable Connection

A+CORE 6.1, OS 4.1

Windows 9x, Windows NT, and Windows 2000 offer a direct cable connection service that allows you to connect two PCs, using either a null modem cable (a cable that connects two PCs using their serial ports) or a parallel cable. When using Windows 9x, follow these directions to use this handy utility (for example, when all you need to do is have two PCs share files or printers, and a cable can reach between them). You can also use this method to allow a guest computer to access shared network resources that a host computer can access.

1. For Windows 98, if it is not already installed, install Direct Cable Connection. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**.
2. Click the **Windows Setup** tab.
3. Select **Communications** and click **Details** (see Figure 17-18). Select **Direct Cable Connection** and check it if it is not already checked.
4. Once a connection is made, install Windows 9x File-and-printer-sharing component so you can share files and printers. To install this network component, click **Start**, point to **Settings**, and click **Control Panel**.
5. Double-click the **Network** icon. Select the **Configuration** tab. If File and printer sharing for Microsoft Networks is not already installed, click **Add**.
6. Select **Service** from the list of components. Click **Add**.
7. From the list of network services, select **File and printer sharing for Microsoft Networks**, and click **OK**. You might be asked to provide the Windows 9x CD-ROM or disks and to restart your computer to complete the installation.
8. After you have installed File and printer sharing, open Windows Explorer. Right-click the drive or folder you want to share, and select **Sharing** from the drop-down menu. Select **Shared as** and click **OK**. A folder that is shared has a hand at the bottom of the folder's icon in Explorer.
9. To use the Direct Cable Connection, click **Start**, point to **Programs**, **Accessories**, **Communications**, and then click **Direct Cable Connection**. The Direct Cable Connection dialog box appears, as in Figure 17-23.
10. You must run Direct Cable Connection on both computers. Select one computer as the host and the other computer as the guest. The host computer will listen for the guest computer. Configure the computer that is to share its resources as the host computer, and the one that is to use these shared resources as the guest computer. Click **Next** to continue.

A+CORE 6.1, OS 4.1

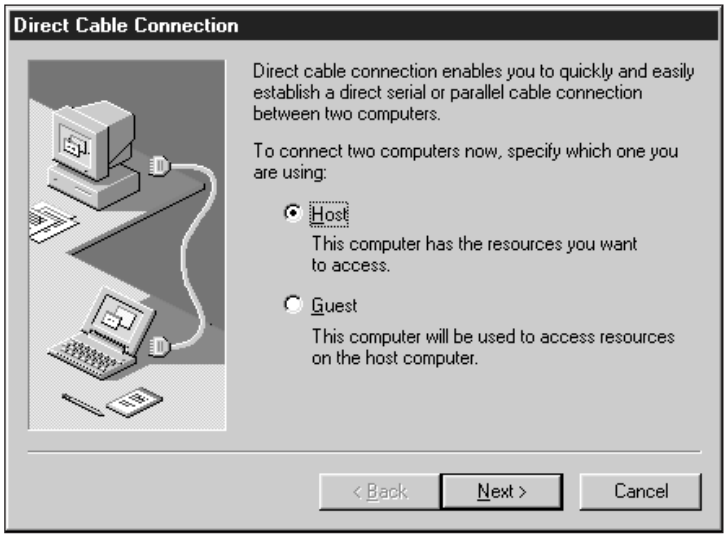


Figure 17-23 Direct Cable Connection is a quick and easy way to connect two computers

11. Select the port you want to use, either a serial port or a parallel port. To use the parallel ports, both computers must have bidirectional parallel ports. Parallel port connections require a parallel cable, and serial port connections require a null modem cable. A printer cable will not work as this parallel cable, because the connection at the printer end of the cable will not fit a PC's parallel port. Buy a parallel cable with two DB-25 male/male connections, or buy an adapter for a printer cable. Connect the cable to both computers and click **Next** to continue.
12. Click **Finish**. For the host computer, the Direct Cable Connection tells you that it is now listening for the guest computer. When you click **Finish** on the guest computer, it attempts to make the connection.
13. After the connection is made, use Windows Explorer on the guest computer to view the shared folders on the host computer. The guest computer can now use resources on the host computer that have been designated for sharing.

Installing Network Adapters Using Windows 9x, Windows NT, or Windows 2000

17

The most powerful and direct access to a network is achieved using a network adapter, or network card. A network adapter may be FDDI, Ethernet, Token Ring, or some other type of network technology. Earlier, the chapter discussed how to select a NIC and configure it. This section moves forward to the next step, installing the NIC using Windows 9x, Windows NT, or Windows 2000.

A+CORE 6.1, OS 4.1

Installing a NIC under Windows NT

Before purchasing a network adapter to be used with Windows NT, check the Windows NT Hardware Compatibility List to make sure that the card is supported by Windows NT. (See Chapter 13 for details of how to do this.) Follow these directions to install a network adapter under Windows NT:

1. Based on information in the card documentation, set DIP switches or jumpers on the card to configure the IRQ and I/O addresses used by the card. Physically install the card in an expansion slot.
2. Turn on the PC and open the Network window: click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Network**.
3. Click the **Adapters** tab. From this tab you can add, remove, and change the settings of adapter cards.
4. Click **Add**. A list of NICs supported by Windows NT appears, as shown in Figure 17-24. Either select the network adapter from the list or click **Have Disk** if your adapter is not in the list and you have on disk the drivers that are designed to work under Windows NT. If you select an adapter from the list, you are asked to supply the location of the Windows NT CD-ROM and the location of files on the CD. For example, if your CD-ROM drive is drive E, type E:\i386. (The folder i386 is used for Intel-based processors.)

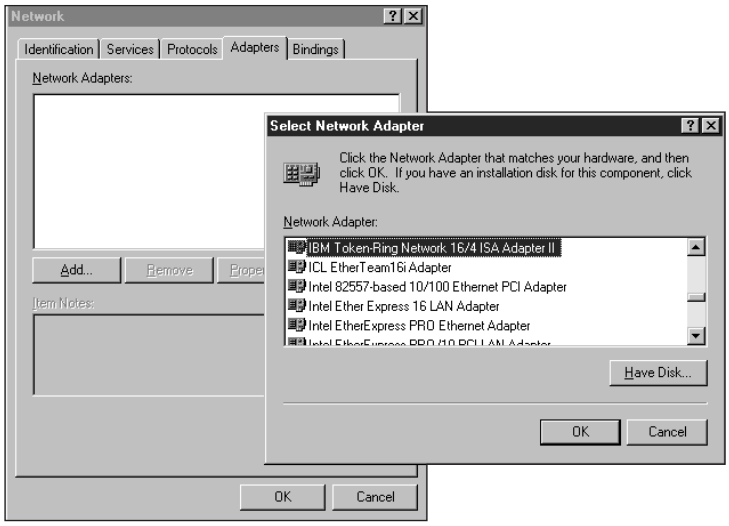


Figure 17-24 Selecting a network adapter supported by Windows NT

5. Windows NT then displays a dialog box (see Figure 17-25) showing the suggested resources to be assigned to the card. You need to know the type of cabling connected to the card and the IRQ and I/O address that the card is configured to use. Click **OK** when you're finished.

A+CORE 6.1, OS 4.1

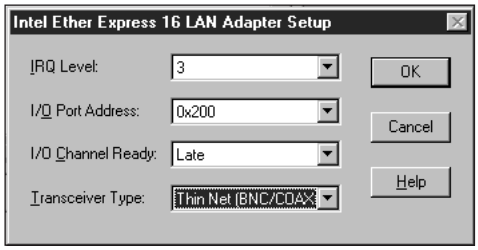


Figure 17-25 Assigning resources to a network card under Windows NT

6. If Windows NT recognizes that the PC has more than one bus, it asks you to select the bus that you are using for the card (as determined by the expansion slot you used). Do so and click **OK**. The card will now be listed under the Adapters tab as an installed card. Reboot the PC.

Installing a NIC Under Windows 9x

Windows 95 supports Ethernet, Token Ring, and ARCnet networking cards. Windows 98 supports ATM, Ethernet, Token Ring, FDDI, IrDA (Infrared Data Association standards for infrared communications), and ARCnet networking cards. In most situations, Windows 9x detects a network card when the PC is first turned on, and automatically configures the card for you. However, for legacy cards you can configure the adapter settings yourself using the Control Panel, as follows:

1. Set DIP switches or jumpers and physically install the network card in the PC. If the card is Plug and Play, it most likely will not have jumpers or DIP switches to set.
2. Turn on the PC. Windows 9x detects the new device and configures it for you. You can check the settings by using the Control Panel: click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Network**.
3. Select the **Configuration** tab. The network card should be in the list of installed network components.
4. Select the card from the list and click **Properties**. Figure 17-26 is displayed.
5. The IRQ and the I/O address of the card are showing. If this is not a Plug and Play card, and you know what the card DIP switches and jumpers are set to, you can compare those values to the values shown here. If Windows 9x did not make a correct match, you can change the settings now. From Configuration type, select **Basic Configuration**, so that you can change the IRQ and I/O address settings. Click **OK** when done.
6. Click **OK** again to save your changes. Reboot the PC to give the NIC its best opportunity to synchronize with the network.

A+CORE 6.1, OS 4.1

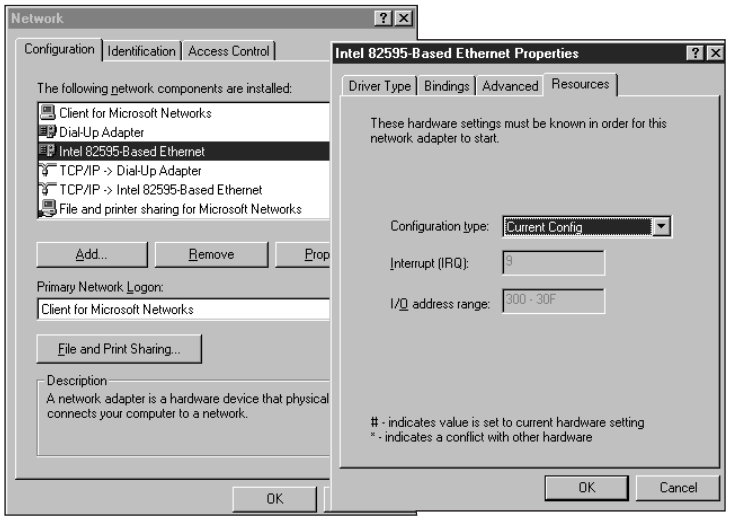


Figure 17-26 A network adapter's resources show in the properties option of the network window

If a network card cannot make a successful connection to the network, the problem might be an IRQ conflict. Try disabling PCI bus IRQ steering (use Device Manager). For more information on resource conflicts under Windows 9x, see Chapter 12.

Installing a NIC Under Windows 2000

After the card is physically installed and the PC is turned on, Windows 2000 automatically detects the card and guides you through the process of installing drivers. After the installation, verify the card is installed. One way to do so is by using Device Manager. To access Device Manager from the Windows 2000 desktop, right-click the **My Computer** icon and select **Properties** from the drop-down menu. The System Properties dialog box opens. Click the **Hardware** tab and then click the **Device Manager** button. The network card should be listed under Network adapters. Right-click the card and select **Properties** to view the card's properties. Another way to access the NIC Properties dialog box is from the Control Panel. Open the **Control Panel** and double-click the **Network and Dial-up Connections** icon. When the dialog box opens, right-click the Local Area Connection icon and select **Properties** to view the card's properties. If you make changes to the properties, reboot the PC.

Using Resources on a Network

You have learned how to access a network either by way of a network card or by way of Dial-Up Networking. After gaining access to the network, software is needed to manage the interface between the network and the OS. This software layer, called network client software, is responsible for determining how your computer will make use of the network protocols to initiate and maintain communication. Windows 2000, Windows NT, and Windows 9x provide client software for several networks, or you can use third-party software. When you

A+CORE 6.1, OS 4.1

install this client software as an add-on component to the OS, the OS provides the Network Neighborhood icon on the desktop. (Windows 2000 calls this icon My Network Places.) Using Network Neighborhood or My Network Places, you can access printers, servers, other PCs, and other resources on the network.

The directions below describe how to install client software that is bundled with Windows 98. This Windows 98 computer is connected to a Microsoft Windows NT network. Follow these directions:

1. Click **Start**, point to **Settings**, and click **Control Panel**. Double-click **Network**. The Network window in Figure 17-27 appears. If client software is already installed, it is listed under installed components. (Note that none is listed in Figure 17-27, so we will add it.)

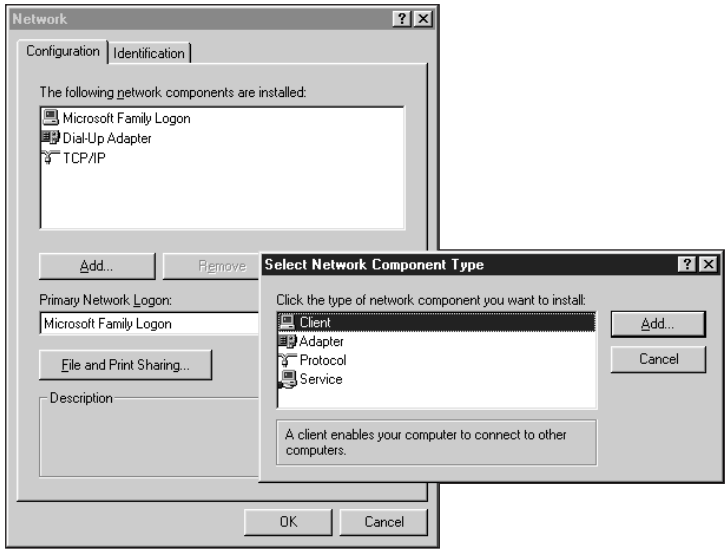


Figure 17-27 Use the Network window of Control Panel to install client software so that the PC can use resources on a LAN

2. Click **Add**. The Select Network Component Type dialog box appears, as shown in Figure 17-27. Select **Client** and click **Add**.
3. The list of network manufacturers that Windows 98 supports is displayed (see Figure 17-28). Notice that Windows 98 supports three network manufacturers: Banyan, Microsoft, and Novell. For a Microsoft Windows NT network, select **Microsoft** as the manufacturer on the left, and **Client for Microsoft Networks** on the right as the network. Click **OK** to continue. Click **OK** a second time to close the Network window. You will be prompted to restart your computer before changes will take effect.

A+CORE 6.1, OS 4.1

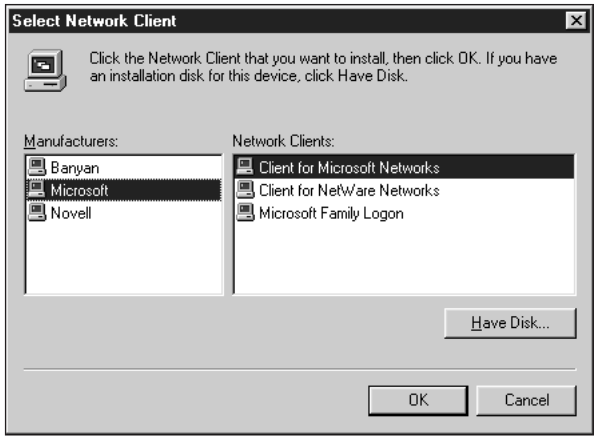


Figure 17-28 Windows 98 supports networks from three manufacturers; network client software must be installed to use these networks

4. After the installation is completed, Client for Microsoft Networks appears as an installed network component, as seen in Figure 17-29. Also notice in the figure that a new icon has appeared on the desktop: Network Neighborhood. Use this icon to access resources on the LAN. When you double-click the icon, the Network Neighborhood window opens, showing available network resources.

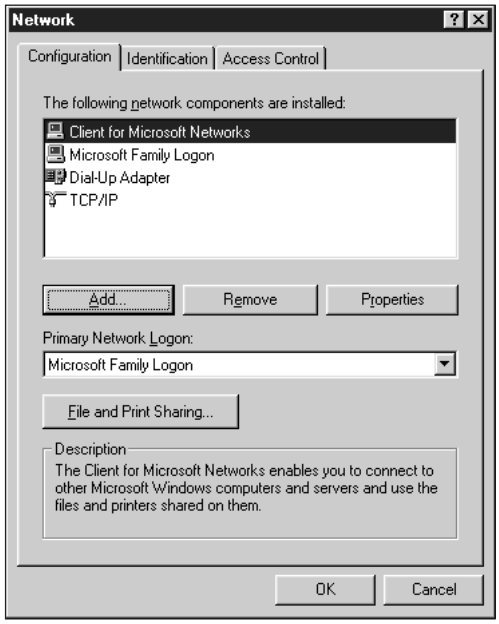


Figure 17-29 After Network client software is installed, it is listed in the Network window and the Network Neighborhood icon appears on the desktop

Servicing PCs on a Network

As a PC technician, you will be expected to troubleshoot and repair PCs connected to networks. You will need to know how to recognize that a PC is connected to a network and how to verify that the connection is working. If the local hard drive loses data or is replaced, you will need to know how to recover the network configuration that was originally on the drive. When the repair is made, you must restore the PC to the network and verify that the connection is again working. Below are general step-by-step directions for a typical situation in which you must remove a PC from a network, make repairs, and then restore the PC to the network.

A network administrator is responsible for the network configuration on the PC and is your resource for specific questions about the network. If, while repairing the PC, you lose the network software and configuration data, work with the network administrator to restore them. Also, when the repairs are made and you are ready to test the network connection, the PC must be logged back on to the network with a valid user ID and password. The PC's end user will have that information. If he or she is not available, see the network administrator.

The steps to disconnect a PC from a network, repair the PC, and reconnect it to the network with the least possible disturbance of the network configuration are summarized in this section:

1. If possible, verify that the PC is network-ready.
2. Log off the network.
3. Save the network files and parameters to disk if you think you might destroy them on the hard drive as you work.
4. Disconnect the network cable and repair the PC.
5. Restore the network configurations.
6. Reconnect the PC to the network.
7. Verify that network resources are available to the PC.

Step 1: Verify That the PC Is Network-Ready

A PC is network-ready if a NIC and client software are installed and the software is configured for a network connection. When you first arrive on-site, check if the PC is connected to a network (look for an installed NIC with an attached cable). Even if a network cable is not attached, the PC might still have network client software installed and configured. If the PC is not working, but the hard drive information is still intact, you can look on it to determine if the PC has client software installed. If the hard drive needs replacing or reformatting, you still might be able to save network configuration information to disk, to make restoring the PC to the network easier.

To verify that a PC is network-ready for DOS and possibly for Windows 9x, look for entries in the CONFIG.SYS and AUTOEXEC.BAT files that execute network software. Also, look in File Manager or Explorer for a network drive. (Remember that a network drive is space

on a network server that appears to be a logical drive on the PC.) Common drive letters for network drives are F or J. If you double-click the drive in File Manager or Explorer and see a list of folders available on the server for this PC, the PC is connected to a network.

For Windows 9x, look for a Network Neighborhood icon on the desktop. Double-click the icon to open the Network Neighborhood window. Double-click the Entire Network icon to see resources on the network that are available to this PC.

Step 2: Log Off the Network

Before you turn off a PC connected to a network, it is important to actually issue the logoff command so that the current session is properly terminated at the network server. If you simply turn off the PC without first logging off the network, the network session may not immediately be terminated. Then, if the user attempts to log on to the network again after the reboot, the user's new session may not be allowed, since the network server thinks there is still an active session.

To log off using NetWare by Novell, Inc. (the most popular LAN software for DOS and Windows 9x systems), access a DOS command prompt and type LOGOFF and press enter. For Windows NT systems, press CTRL-ALT-DEL and choose logoff from the dialog box that appears.

Step 3: Save the Network Files and Parameters to Disk

Because the most popular network software for DOS and Windows 95 PCs is Novell, the files, commands, and data used by Novell are described below. Novell and Windows NT networking software is also described for Windows 98 and Windows NT workstations.

Using DOS or Windows 95 NetWare by Novell uses entries in CONFIG.SYS and AUTOEXEC.BAT for DOS and Windows 95, to load network software and drivers and to provide a logon screen for the user to log on to the network. You will want to preserve these entries without changes to restore the network connection after the repair. The NetWare software, by default, is located in the directory \NWCLIENT, although another directory name can be used. Expect to see four to six command lines in the AUTOEXEC.BAT file placed there by NetWare or by the network administrator, and one command line in CONFIG.SYS. The one entry in CONFIG.SYS is LASTDRIVE=Z: (or some other letter), which allows for network drive letters.

An example of a group of startup commands for NetWare that typically might be found in AUTOEXEC.BAT is shown below:

```
SET NWLANGUAGE=English
C:\NWCLIENT\LSL.COM
C:\NWCLIENT\3C5X9.COM
C:\NWCLIENT\IPXODI.COM
C:\NWCLIENT\VLM.EXE
F:\LOGIN JANDREWS
```

The commands might be grouped together in AUTOEXEC.BAT, and preceded by remarks indicating that they are used to load the client software. IPXODI.COM and VLM.EXE (lines 4 and 5 above) are the two main programs of the NetWare client software. The third line above loads a driver for the network card. Sometimes the command lines will include LH at the beginning of the command line, to cause the program to load into upper memory.

The last command line in the list provides a logon screen for the user. The username is included in the command line (JANDREWS in this example) so that the user only needs to enter his or her password. The username can be omitted in the command line and entered from the prompt. The F:\ at the beginning of the command line tells NetWare to access the NetWare server to run the logon program to log on to the network. Figure 17-30 shows the results after entering the command LOGIN without the username included. (Different versions of NetWare may have different login boxes than the one shown in the figure.) The user enters the username and password just as they are recorded on the NetWare server.

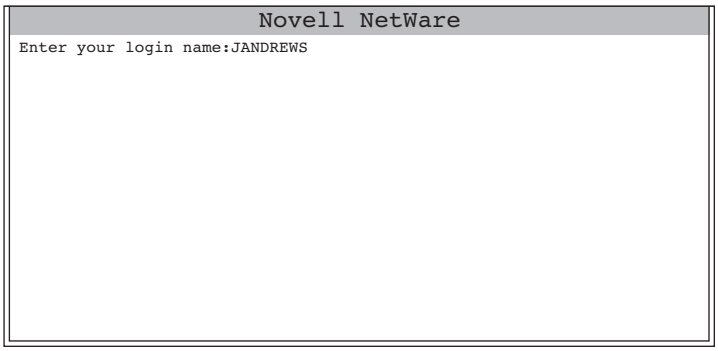


Figure 17-30 Netware provides a logon screen to log on to a Novell LAN

Sometimes you will see the command lines listed above stored in a batch file, and the batch file referenced in AUTOEXEC.BAT. For example, a batch file named START.BAT might be in the \NWCLIENT directory, and the command C:\NWCLIENT\START in the AUTOEXEC.BAT file.

You may need to replace or reformat the hard drive. If so, be sure to preserve the network settings. The easiest way to do this is to back up the CONFIG.SYS and AUTOEXEC.BAT files, including the network commands. In addition to these two files, one important file in the \NWCLIENT directory is NET.CFG, which contains the specific network configuration information for this PC. If you are having problems with the hard drive, but you have the opportunity to save just a few files, consider this one file important, because it contains information specific to this PC's network configuration.

Using Windows 98, Windows NT, Windows 2000 You can connect a Windows 98, Windows NT, or Windows 2000 workstation to a network in two ways: using the client software included with Windows, or using client software from Novell or some other third-party network client. For a Windows NT workstation on a Novell NetWare network, if Microsoft's Windows NT client software is used instead of Novell's, then you will see the CSNW

(Client Service for NetWare) icon in the Control Panel. For a Windows 2000 workstation using CSNW on a NetWare network, look for CSNW installed under the Network and Dial-Up Connections icon in Control Panel. If Microsoft's Windows 98 client software for Novell is used, look for Novell NetWare as an installed network component in the Network window under Control Panel. In any case, if the hard drive of a PC using one of these OSs looses the client software installation, ask the network administrator for assistance to reinstall either the Windows or Novell client software. It will not be possible to simply copy files back to the hard drive, as with DOS or Windows 95, because Windows 98, Windows NT and Windows 2000 store network settings in the Registry.

Step 4: Disconnect the Network Cable and Repair the PC

After you have logged off the network and saved configuration information to disk, disconnect the network cable (called a patch cable) and repair the PC. If you must exchange the NIC, use an identical card with identical jumper and DIP switch settings, because the drivers on the PC are set up specifically for this card. If you are exchanging one type of NIC for another, ask the network administrator to help you reconfigure the PC for the new type of card.

Step 5: Restore the Network Configurations

Reboot the PC without reconnecting the network cable, and restore the network files and parameters, including the commands in CONFIG.SYS and AUTOEXEC.BAT for a DOS or Windows 95 PC, to load the network software and provide a logon screen. The network administrator may provide you with network software to reinstall, or may simply ask you, for a Novell network, to restore the \NWCLIENT directory together with the OS startup files, CONFIG.SYS, and AUTOEXEC.BAT. For Windows 2000, Windows NT, or Windows 98, ask the network administrator to help reinstall the network software.

Step 6: Reconnect the PC to the Network

Turn the PC off, reconnect the network cable, and then turn the PC back on. When the PC boots, the network software should load, and a logon screen should be displayed to reestablish a network session. If you are rebooting the PC with NetWare, the login screen in Figure 17-30 appears. Have the user log on to the network with his or her user ID and password, or use one provided to you by the network administrator for testing. NetWare displays a message saying that you are logged on, and then Windows is loaded.

For DOS and Windows 95, if the network software loads, but the logon screen does not appear, you can issue the LOGIN command from the command prompt. Just enter the command as it appears in the AUTOEXEC.BAT file. For Windows 2000, Windows NT, and Windows 98, if the workstation is connected to a Microsoft network, the logon to the workstation will also log the workstation on to the network. For NetWare networks, the logon may be two different logons, one to the workstation and the other to the NetWare network, or the logon may be synchronized so that both logons occur simultaneously.

Step 7: Verify That Network Resources Are Available to the PC

To verify that all is well with the network, look in Explorer and verify that the network drive is present. Look for drive F or drive J, or some other drive letter representing a network drive. You can find the network drive letter by looking either in AUTOEXEC.BAT at the LOGIN command, or at the contents of NET.CFG in the \NWCLIENT directory for a NetWare network. Network drives are covered in more detail later in the chapter. For Windows NT and Windows 98, check Network Neighborhood for networking resources to determine if the network is functioning correctly. For Windows 2000, check My Network Places. If you don't find resources there, try rebooting the PC.

PCs and the Internet

A+ OS 4.2

The **Internet** is the largest network in the world. To be more accurate, it is the largest grouping of many networks internetworked together. The software and protocols used by the Internet include all the OSI layers from the application layer through the network layer (see Figure 17-14). At the foundation of the Internet is TCP/IP, which operates at the OSI transport and network layers. TCP/IP was developed in 1969 by the U.S. Department of Defense (DOD) to provide a decentralized and fast network to connect networks. The network was originally called ARPANET (Advanced Research Project Agency network), from which the civilian Internet evolved. DOD wanted decentralized data transfers so that communication would not be dependent on any one server or network, backbone network, or centralized geographic location in order to function. This decentralized concept means that, even if many networks fail, data will still arrive at its destination. Originally, this design was intended to protect data communications in case of a major military attack on the United States, in which many networks might be put out of service. Another goal of decentralization was to allow any one communication to travel from source to destination through any number of different paths, or to be broken into parts that travel different paths, and come together at their single destination.

The Internet is a web of interconnecting, yet independent, networks. Many people confuse the Internet with the World Wide Web (WWW). Again, note in Figure 17-14 that the Web operates at the OSI application and presentation layers and is only one service of many services that use TCP/IP. The Web presents data to Internet users as pages—called web pages—displayed on computer monitors. These pages of information can contain graphics and texts with links to sound files, video files, animation, all types of graphics, other web pages, and other programs. The Web is only one way to communicate over the Internet at the user, or application, level. Other ways, also shown in Figure 17-14, are chat rooms, e-mail, and FTP.

The Internet is a network of networks, and TCP/IP is designed to work in a mixture of several types of networks. Underneath TCP/IP is some other protocol such as PPP, Ethernet, Token Ring, or FDDI, providing the bottom two layers of the OSI model (again, see Figure 17-14). TCP/IP enables packets of data to traverse many networks to arrive at their destination. To understand how these packets can be routed all the way around the world is to understand TCP/IP. One way of looking at this relationship between TCP/IP and network protocols at the

A+ OS 4.2

data-link and physical layers is to consider that the Internet, using TCP/IP, uses these underlying networks like a shipping department uses different transportation systems. For example, a package is shipped first by truck, then by train, then by plane, and again by truck before arriving at its destination. In this analogy, TCP/IP is like the shipping box that encloses the contents and the mailing label that identifies the package, its sender, and its destination to all the subsystems sending it on its way. The subsystems are the protocols in the data-link and physical layers of the OSI model.

How the Internet Works

Figure 17-31 shows a simplified, bird's-eye view of how networks work together to send data over the Internet. A user in California accesses a server in New York by traversing many networks. Each network operates independently of all other networks but can also receive a packet from another network and send it on to a third network, while it also manages its own routine, internal traffic. Networks are connected by routers, which belong to more than one network. In Figure 17-31, Network B contains four routers: Routers 1, 2, 3, and 4. But Routers 3 and 4 also belong to Network C. Network C contains Router 8, which also belongs to the same network as the server in New York that the user wants to access.

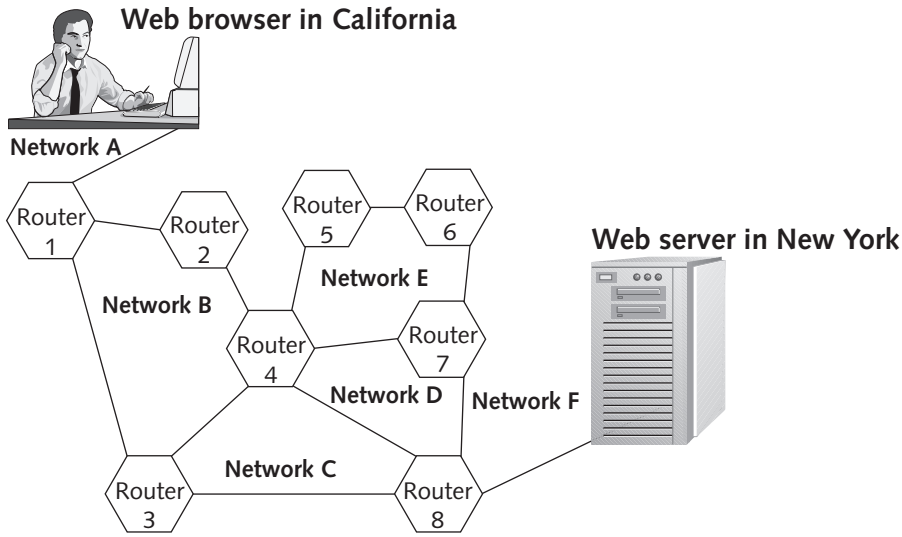


Figure 17-31 The Internet is a web of interconnecting, yet independent, networks

How many paths are there on the Internet by which the user in California can access the server in New York? One path is through Router 1, then 3, then 8, and finally to the server. Data going from the server to the user may travel a different path than data traveling from the user to the server. In fact, if there is a lot of data divided into several packets, each packet may take a different route, and the packets may not arrive at the user's PC in the same order in which they were sent. It's up to the lower layers in the OSI model to sort it all out and reassemble the data before it's presented to the application layer to be presented to the user.

Connecting to the Internet

A+ OS 4.2

There is a variety of ways for a PC to access the Internet. Most people access the Internet through an **Internet service provider** (**ISP**). For a monthly fee, the service provider gives you a username and password, and an access phone number, and may include necessary software for your PC. In addition to providing access to the Internet, the larger ISPs also provide online services, an infrastructure that enables subscribers to communicate with one another, to get stock quotes and news, and to use community bulletin boards. The largest ISPs that also provide online services are America Online, Microsoft Network, and CompuServe. For a listing of over 3000 ISPs, see the web site *www.thelist.internet.com*.

In Figure 17-31, a router that belongs to a network has a network address on that network. However, a router can have more than one network address. Router 4, in the diagram, belongs to four networks (B, C, D, and E), and would, therefore, have four network addresses. On the Internet, each device that can be addressed by TCP/IP is assigned a combination address containing both the network address (which identifies the network) and the host address (which identifies the individual device or computer). (More about network and host addresses below.) This combination address is called an **Internet Protocol address** (**IP address**). A host on the Internet is defined as any computer or device that can have an IP address. Therefore, in Figure 17-31, Router 4 is a host that has four IP addresses. The network portion of each IP address corresponds to each of the four networks it belongs to, and the host portion of each IP address is unique for the given network.

This section looks at the basics of the Internet, how IP addresses on the Internet are determined, how TCP/IP uses these IP addresses to route data, and the details of connecting a PC to the Internet.

IP Addresses

The Internet and the UNIX operating system use Transmission Control Protocol/Internet Protocol (TCP/IP) as their network protocol. TCP/IP requires that each node on a network be assigned a unique numeric address, called an IP address. The organization that keeps track of all IP address assignments is Network Solutions, Inc. (NSI), working under an agreement with the National Science Foundation. The work is done at the **Internet Network Information Center** (**InterNIC**) in Menlo Park, California. When a company, college, or some other organization applies for IP addresses, InterNIC assigns a range of addresses appropriate to the number of hosts on the organization's networks. For more information about InterNIC, see its web site, *www.internic.com*.

An IP address is 32 bits long, made up of four 8-bit numbers separated by periods. The largest possible 8-bit number is 11111111, which is equal to 255 in decimal, so the largest possible IP address in decimal is 255.255.255.255. Each of the four numbers separated by periods is called an **octet** (for 8 bits) and can be any number from 0 to 255, making for a total of 4.3 billion potential IP addresses (256 x 256 x 256 x 256). (However, because of the allocation scheme used to assign these addresses, not all of them are readily available for use.)

Classes of IP Addresses

IP addresses are divided into three classes—Class A, Class B, and Class C—based on the number of possible IP addresses in each network within each class. IP addresses are assigned to these classes according to the scheme outlined in Table 17-3. A Class A license assigns a single number to be used in the first (leftmost) octet of the address, which is the network address. (The first bit of the first octet for a Class A IP address is always zero.) The remaining three octets of the IP address can be used for host addresses that uniquely identify each host on this network. The first octet of a Class A license is a number between 0 and 126. For example, if a company is assigned 87 as its Class A network address, then 87 is used as the first octet for every host on this one network. Examples of IP addresses for hosts on this network are 87.0.0.1, 87.0.0.2, and 87.0.0.3 (the last octet does not use 0 or 255 as a value, so 87.0.0.0 would not be valid). Therefore, one Class A license can have approximately 256 2 256 2 254 node addresses, or about 16 million IP addresses.

Table 17-3 Classes of IP addresses

Class	Network Octets (blanks in the IP address are used for octets identifying hosts)	Total Number of Possible Networks or Licenses	Host Octets (blanks in the IP address are used for octets identifying networks)	Total Number of Possible IP Addresses in Each Network
A	0.___.___.___ to 126.___.___.___	127	___.0.0.1 to ___.255.255.254	16 million
B	128.0.___.___ to 191.255.___.___	16,000	___.___.0.1 to ___.___.255.254	65,000
C	192.0.0.___ to 254.255.255.___	2,000,000	___.___.___.1 to ___.___.___.254	254

A Class B license assigns a number for each of the first two leftmost octets, leaving the third and fourth octets for host addresses. (The first two bits of the first octet for a Class B IP address are always 10.) The number of possible values for two octets is about 256 2 256 (some IP addresses are reserved, so these numbers are approximations), or about 65,000 host addresses in a single Class B license. However, the first octet of a Class B license is a number between 128 and 191, which gives about 63 different values for a Class B first octet. The second number can be between 0 and 255, so there are approximately 63 2 256, or about 16,000, Class B networks. For example, suppose a company is assigned 135.18 as the network address for its Class B license. The first two octets for all hosts on this network are 135.18, and the company uses the last two octets for host addresses. Examples of IP addresses on this company's Class B network are 135.18.0.1, 135.18.0.2, 135.18.0.3, and so forth.

A Class C license assigns three octets as the network address. (The first three bits of the first octet for a Class C IP address are always 110.) With only one octet used for the host addresses, there can be only 254 host addresses on a Class C network. The first number of a Class C license is between 192 and 254. For example, if a company is assigned a Class C license for its

network with a network address of 200.80.15, some IP addresses on this Class C network would be 200.80.15.1, 200.80.15.2, and 200.80.15.3.

When a small company is assigned a Class C license, it obtains 254 IP addresses for its use. If it only has a few nodes (say, less than 25 on a network), many IP addresses go unused, which is one of the reasons that there is a shortage of IP addresses. If the company grows and now has 300 workstations on the network, it runs out of IP addresses. Most companies solve this problem by assigning their own private IP addresses. The following IP addresses are not used on the Internet and can be assigned to any private network:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

How does a PCs with private IP addresses access the Internet? By making its request to a server that communicates with the Internet on its behalf, using its own public IP address for the request. This server is called a **proxy server** and uses a method called **Network Address Translation (NAT)**. Hosts on the Internet only communicate with this one proxy server instead of every PC on the private network, which brings a degree of security to the private network. In addition, the entire network requires only a single publicly assigned IP address, which, in many cases, will be assigned by the ISP. Windows 98 SE and Windows 2000 include proxy server software called **Internet Connection Sharing**. One PC must be configured as the proxy server and others on the network are configured to access the Internet through the proxy server.

When assigning private IP addresses to a network, keep in mind that a few IP addresses are reserved for special use by TCP/IP and should not be used. They are listed in Table 17-4.

Table 17-4 Reserved IP addresses

IP Address	How It Is Used
255.255.255.255	Broadcast messages
0.0.0.0	A currently unassigned IP address
127.0.0.1	Indicates your own workstation; yourself

Dynamically Assigned IP Addresses

An IP address permanently assigned to a workstation is called a **static IP address**, but, for a large network, it can become very difficult to manually keep track of each IP address assigned to each PC. Another solution is to have a server automatically assign an IP address to a workstation every time it comes online to the network, using an IP address from a range of IP addresses allotted the service. These IP addresses are called **dynamic IP addresses**.

The server that manages these dynamically assigned IP addresses is called a **Dynamic Host Configuration Protocol** (**DHCP**) server. In this arrangement, workstations are called DHCP clients. DHCP software resides on both the client and the server to manage the dynamic assignments of IP addresses. DHCP client software is built into Windows 9x, Windows NT, and Windows 2000. Many Internet service providers (ISPs) use dynamic IP addressing for their dial-up users.

Plans for New IP Addresses

Because of an impending shortage of IP addresses, a new scheme of IP addresses is currently being developed. Called the IP version 6 (IPv6) standard, it will use 128 bits (four 32-bit segments) instead of 32 bits (four 8-bit segments). Ipv6 will have the added advantage over current IP addressing that it can automatically assign an IP address to a network device.

Domain Names

A+ OS 4.2

Because IP addresses are numbers and sometimes difficult to remember, and because companies might want to change their IP addresses without also changing the name that Internet users recognize, hosts are sometimes given alphabetic, or word-based, names called **domain names**. Domain names are an alternate way of addressing a host on the Internet, but all domain names must eventually be mapped onto a host's IP address before contact with the host can take place. Think of a domain name as a pseudonym or an alias; the real name of the host computer is its IP address.

The last segment of a domain name tells you something about the host. Domain names in the United States end in .edu (for educational institution), .gov (for government institution), .com (for commercial institution), .org (for nonprofit institution), and .net (for Internet provider). There are other endings as well, including codes for countries, such as .uk for the United Kingdom. Examples of domain names are course.com, microsoft.com, and leeuniversity.edu. The enormous demand for commercial domain names, combined with a shortage of acceptable domain names, has led to upcoming new domain name suffixes and longer lengths for domain names.

Domain Name Resolution

There is not necessarily a fixed relationship between a domain name and an IP address. A host computer can have a certain domain name and can be connected to one network and assigned a certain IP address, and then be moved to another network and assigned a different IP address. The domain name can stay with the host while it connects to either network. It is up to a name resolution service to track the relationship between a domain name and the current IP address of the host computer.

Two name resolution services track relationships between computer names and IP addresses. **Domain Name System**, also called **Domain Name Service (DNS)** tracks domain names, and Microsoft's **Windows Internet Naming Service (WINS)**, used only on Microsoft networks, tracks NetBIOS names.

At the heart of DNS is a distributed database, which must initially be updated manually. When a new domain name is assigned, that name and its corresponding IP address are

A+ OS 4.2

entered into a database on a top-level domain name server. When a remote computer tries to access your host by using your domain name, if that remote computer does not know the IP address currently assigned to that domain name, it queries its DNS server. If the DNS server does not have the information in its DNS database, it contacts another DNS server for that information and updates its database. This second DNS server is designated as its top-level DNS server and can contain the initial manual entry into the Internet system that relates a domain name to an IP address. The local DNS server is also informed, and then tells the remote computer the IP address of the domain name.

Recall that when a computer is configured for a network, it is assigned a computer name so that other computers and devices on the network can access this computer without knowing its IP address. Windows 9x and Windows NT assume this name is a NetBIOS name and use WINS as its default name resolution process. If that fails, it turns to DNS to resolve the name. Windows 2000 assumes its computer name is a domain name and uses DNS as its default name resolution process. If that fails, it turns to NetBIOS WINS resolution to resolve the name.

The Internet, Networks, and Subnets

All the networks that make up the Internet use the TCP/IP protocol suite. When you understand how TCP/IP addresses networks and host computers and routes data around the Internet, the task of configuring Windows to connect to the Internet becomes much clearer. This section begins by introducing the many different protocols that make up the TCP/IP protocol suite, and then discusses how TCP/IP uses the IP address system.

Routing Using TCP/IP

TCP/IP uses routers to transfer packets of data from network to network in such a way that the overall transmission makes all these networks appear to be one large network. Each protocol of the TCP/IP suite is designed to perform a single task—such as error checking or sending error messages back to the sending host—as part of the overall stupendous task of routing packets around the world. TCP and IP are the two principal protocols of the suite, but there are others.

The Suite of TCP/IP Protocols TCP/IP can use more than one protocol at each OSI layer that it supports. However, when data is being transmitted, only one protocol is used at each layer. The choice of which protocol to use depends on what type of data is being transmitted and on what applications software is interfacing with the network.

Figure 17-32 shows the protocols of the TCP/IP suite supported by Windows. The Windows Sockets protocol (sometimes called WinSock) is designed to interface with applications that rely on sockets, or sessions, to connect to a remote computer. Browser software for the World Wide Web is one example of software that uses sockets. **NetBIOS over TCP/IP** (**NetBT**) is another applications protocol designed to interface with applications that rely on NetBIOS for communication. There is more information about applications protocols later in the chapter.

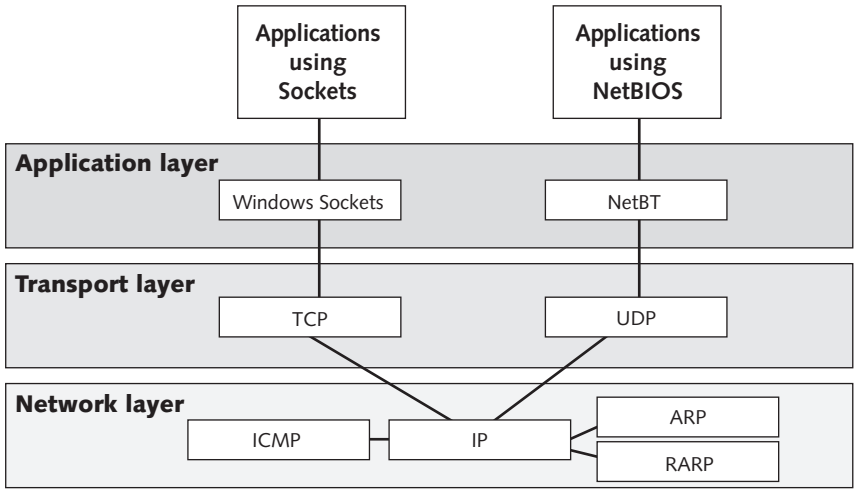


Figure 17-32 Protocols of the TCP/IP suite supported by Windows 9x and Windows NT

There are two protocols at the transport layer, TCP and UDP. **User Datagram Protocol** (**UDP**) is a **connectionless protocol**, meaning that it does not require a connection to send a packet and does not guarantee that the packet will arrive at its destination. UDP is used to send broadcast messages over the network when responses from each node are not required. One service at the application layer that uses UDP is a network drive map, which uses UDP because it does its own verifying that the packets have arrived safely. (A network drive map makes space on a remote computer's hard drive, to look like a hard drive on the local computer.) TCP is a **connection protocol**, meaning that data is guaranteed to arrive at its destination. Most network applications use TCP rather than UDP. To understand the difference in sending data over a network with or without a connection, think of the difference between a radio broadcast and a telephone call. The radio broadcast does not require a connection at the remote end to confirm receipt of the signal. It is therefore, a type of connectionless communication. On the other hand, a telephone call requires a connection at both ends for data to be communicated, and is an example of communication with a connection.

At the network layer, **Address Resolution Protocol** (**ARP**) converts IP addresses into physical network addresses such as Ethernet IDs or Token Ring MAC addresses. A counterpart protocol, **Reverse Address Resolution Protocol** (**RARP**) does the reverse and converts physical network addresses into IP addresses. Also at the network layer is **Internet Control Message Protocol** (**ICMP**), which transmits error messages and other control messages to hosts and routers. For example, if a router is unable to deliver a packet, it informs the sender of the failure using ICMP.

IP Addresses and Physical Addresses Fundamental to the design of TCP/IP is the concept of routing packets across networks by using IP addresses that relate to physical network adapter addresses. The routers of each network are responsible for routing packets from outside the networks to the hosts within their own network. These routers may or may not

know the adapter address of the host but will "learn" the address the first time a packet is sent to it. Other routers outside the network also might know the adapter addresses of hosts within this one network.

Think of IP addresses and adapter addresses as phone numbers and street addresses of houses, respectively, as seen in Figure 17-33. A house on a certain street of a city may have one phone number today, but another one tomorrow if new owners move in, or if the present owner has his or her phone number changed. However, the street and city address of this house will most likely never change.

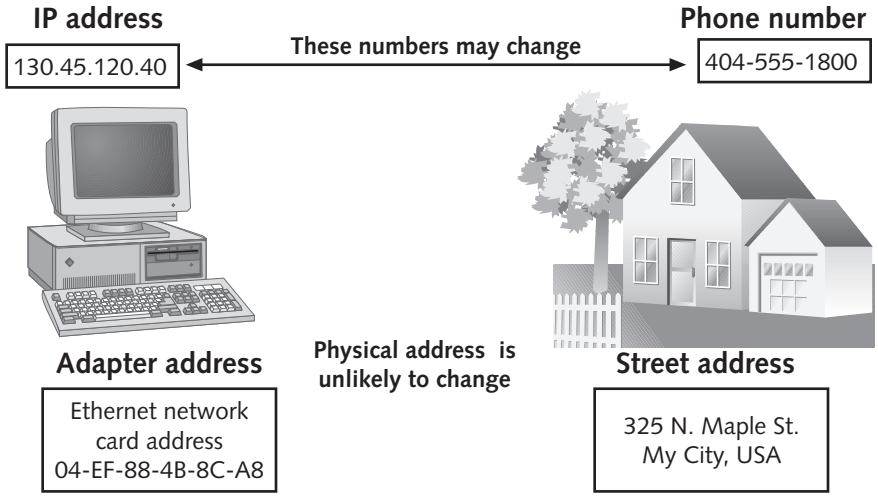


Figure 17-33 IP addresses and physical network addresses can be compared to phone numbers and street addresses

An IP address is assigned to a host just as a phone number is assigned to a house (no inherent relationship), and both the IP address and phone number can easily change. An adapter address is like the physical address of the host and only changes if the network adapter card is exchanged, just as the street address of a house seldom, if ever, changes. Think of adapter addresses as the permanent physical network addresses of hosts.

We can take the analogy one step further. An IP address is made up of a network and host address, just as phone numbers consist of area codes followed by seven-digit numbers. The area code generally identifies the approximate location of the house, just as the network portion of an IP address generally identifies the location of the network where the host resides.

When configuring a workstation to use TCP/IP, one step in the configuration is to associate an adapter address to an IP address. This process is called binding the adapter address to the IP address. When an IP address is bound to the adapter address, TCP/IP data that is addressed to this IP address now has a physical computer or adapter address to send the data to. (In general, the term **binding** refers to associating any OSI layer in the network to a layer just above it or just below it. For example, an application protocol can be bound to a transport protocol,

and a transport protocol can be bound to a network protocol. When the two layers are bound, communication continues between them until they are unbound or released.)

How TCP/IP Routing Works Figure 17-34 shows an example of two TCP/IP networks connected by a router. The router (Computer C) belongs to both networks and has an IP address for each network. Think of it as the intersection point of the two networks.

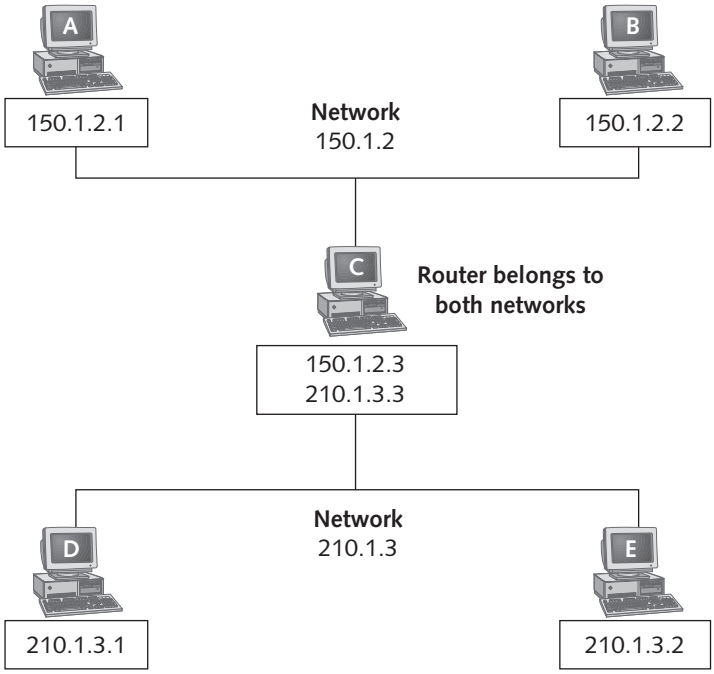


Figure 17-34 Two networks using TCP/IP connected by a router

Suppose both these networks are Ethernet, and Host A wants to send data to Host B, which is on the same network. Host A knows the IP address of Host B. It would also need to know the Ethernet address (adapter address) of Host B in order to send the packet. This is what happens:

1. Host A knows the Host B IP address and turns the job of discovering the adapter address over to ARP (Address Resolution Protocol), which looks up the IP address of Host B in its routing tables on the Host A PC.
2. If ARP does not find the IP address of Host B in its tables, it sends out a broadcast message to the entire network (Hosts B and C in this case), containing a request for the adapter address of Host B.
3. Host B recognizes its IP address and responds with its Ethernet adapter address.
4. Host A receives the packet and updates its routing tables.
5. Host A sends its packet to Host B.

Now suppose that Host A is now ready to send a packet to Host E, which is on the other network. Here's what happens:

1. Host A looks at the IP address of Host E and recognizes that Host E does not belong to its network. (How it recognizes that is coming up.)
2. Because Host A is trying to communicate with a different network, it sends the packet to the router of its network, in this case, Host C. Host A knows the Ethernet address of its router, so it knows where to send the packet. (Host A did not attempt to broadcast for a response from Host E because it recognized that Host E would not hear the broadcast message, since it is on a different network.)
3. Host C receives the packet and looks at the destination IP address. Host C recognizes that the destination IP address is on its second network, so it sends the packet to Host E, just as Host A sent the packet to Host C. In other words, it will first look in its router table. If it doesn't find the IP address of Host E, it will send out a broadcast message to Host E's network.

Also note that in this example, Host C is an IP router but is also called a gateway, because it serves as the connection point of two networks.

Default Gateways Sometimes a large network will have more than one router, as seen in Figure 17-35. The network in the upper left of the figure is 250.1.2 and has two routers (D and E), each belonging to other networks. Host E is designated as the **default gateway**, meaning that hosts on the 250.1.2 network will send packets addressed to other networks to this gateway first. The other router, Host D, is called the **alternate gateway** and will be used if communication to the default gateway fails.

Suppose Host A on network 250.1.2 wants to send a packet to Host K on Network 210.1.3 in the figure. Host A first sends its packet to the default gateway. If that fails, Host A will try the alternate gateway. Sometimes the default gateway knows that a packet should be routed through an alternate gateway. If so, it will send an ICMP redirect packet back to Host A, telling Host A to use the alternate gateway when addressing Host K. The next time Host A attempts to send a packet to Host K, it reads from its routing table to use the alternate gateway.

Network Mask Comparing the network addresses in Figure 17-35 to those of Table 17-3, you can see that networks 250.1.2 and 210.1.3 are Class C networks, and network 130.5 is a Class B network. Also remember that Host A had to determine that Host K was not on its network, but was on a foreign network. How did it know that? By comparing Host K's IP address to the network mask. A **network mask** is that part of the IP address that identifies the network rather than the host. Host A's network address is 250.1.2. Host A compared these values to the first three octets of Host K's IP address. Since they were not the same, Host A knew that Host K was on another network.

Also notice in Figure 17-35 that the three network addresses are 250.1.2, 210.1.3, and 130.5. The first two networks are Class C networks because three octets are used in the network address, and the third network is a Class B network because the network address only has two octets. You can also identify the class of a network address by the first number; 250 and 210 fall within the range for Class C addresses, and 130 falls within the range of a Class B address.

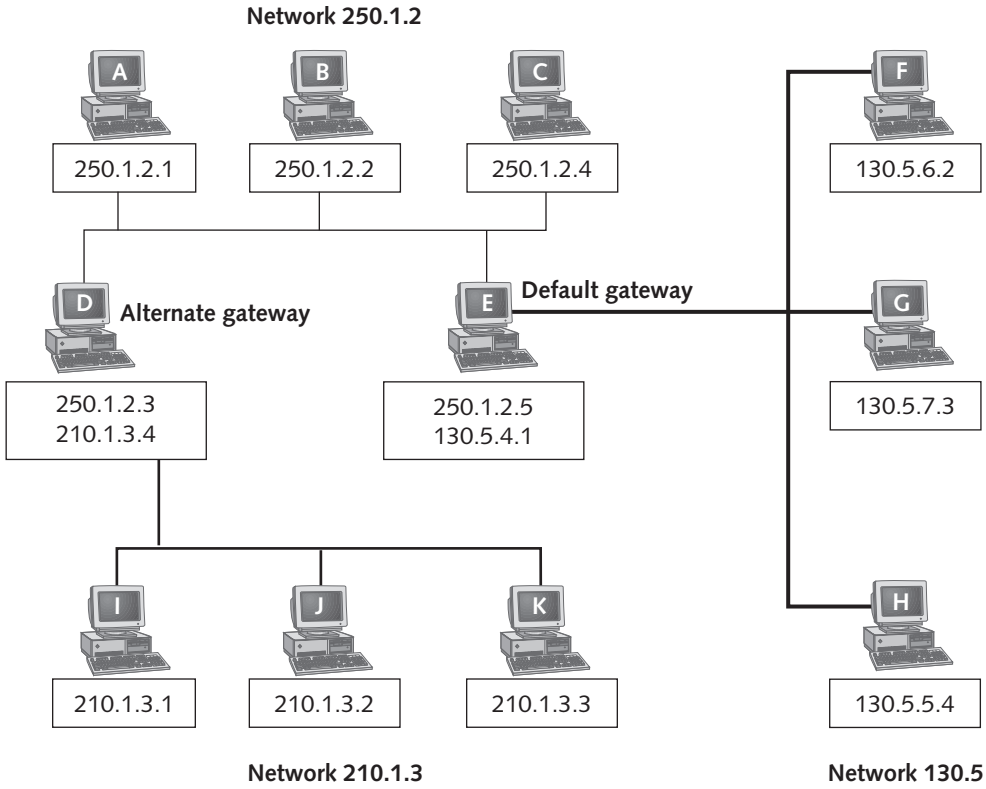


Figure 17-35 A network can have more than one router; one router of the network will be the default gateway

Subnets

In configuring TCP/IP on a workstation, besides entering the IP address, you must also enter one or more subnet masks. A **subnet mask** looks like an IP address because it has four numbers separated by periods, but it is not an IP address. It's a number that defines which portion of an IP address identifies the network (including the subnet) and which portion identifies the host. (It does not contain a network address; that's in an IP address.)

Remember, from our earlier discussions in the chapter, that an IP address contains two parts, a network address and a host address. When a large company applies for a single class license, it is assigned a single network address from which it can create many IP addresses unique to each host in its network. The company may have many networks, and many workstations within these networks need these IP addresses. In order to take full advantage of the routing abilities of TCP/IP, each of these networks is assigned a group of IP addresses within the one class license. Each group is called a **subnet**. A single Class A, B, or C license can be divided into several subnets. Each subnet is a network segment or single network of the company. Traffic can be better controlled using subnets because local traffic can be contained within its own subnet and routers can be effectively used to route traffic from subnet to subnet.

TCP/IP can manage this by using not only network addresses, but subnet addresses as well. A few bits at the beginning of the host portion of the IP address are borrowed from the host and used to identify the subnet, and the subnet mask tells how many of these bits are used for that purpose. An example of a subnet mask is 255.255.240.0. When converted to bits, it looks like this: 11111111.11111111.11110000.00000000.

All subnet masks, when converted to bits, will have all ones on the left and all zeroes on the right. The ones define the network portion (including the subnet) of the mask, and the zeroes define the host portion. A host uses its subnet mask to decide if a destination host is in its subnet. It determines how many bits in a destination IP address belong to the network address by the number of ones in its subnet mask. Once it knows what portion of the destination IP address is the network address, it compares that portion of the address to its own address to decide if the destination address is inside its own subnet. If it is, it will attempt to communicate with it directly. If the IP address is outside its subnet, it will communicate through the router.

Let's look at one example, using these values:

- Sending IP address: 130.5.206.189
- Destination IP address: 130.5.194.5
- Subnet mask: 255.255.240.0

Here's what the sending host does:

1. The sending host IP address, the destination host IP address, and the subnet masks are all converted to bits:

   Sending IP address: 130.5.206.189 = 10000010.00000101.11001110.10111101

   Destination IP address: 130.5.194.5 = 10000010.00000101.11000010.00000101

   Subnet mask: 255.255.240.0 = 11111111.11111111.11110000.00000000

2. From the subnet mask, the host knows that the first 20 bits of the IP addresses are the network address so it only uses those bits to make the comparison between its IP address and the destination IP address:

   Sending IP address, network portion: 10000010.00000101.1100

   Destination IP address, network portion: 10000010.00000101.1100

3. The network portions of the two IP addresses are the same, so the sending host attempts to communicate directly with the destination host.

When configuring a computer for TCP/IP using static IP addressing, remember that the PC must know the subnet mask to determine if an IP address it wants to communicate with is inside or outside its subnet.

WAN Connections

A company that supports a WAN often uses subnets to help manage a group of networks, each with its own network technology. It is also common for every PC on a WAN to need

access to the Internet although not all individual networks in the WAN have this direct connection. A company might not own an entire Class A, Class B, or Class C license, but might lease IP addresses from an ISP. This section looks at how a small WAN might be configured to manage these possibilities.

When a service provider owns several Class C network addresses and subleases or subnets them to small companies, these addresses are called **classless addresses** because they are used on networks with subnet masks that don't fall on full octets. The service provider might also lease out an IP address that serves as a gateway to the Internet. This static IP address on a server at the ISP will belong to a subnet at the company site. For example, in Figure 17-36, a small organization has two networks, a Token Ring and an Ethernet. It leases IP addresses from an ISP with an ISDN direct line to an Internet gateway to the ISP. The company uses a subnet mask of 255.255.255.192 (11111111.11111111.11111111.11000000) so that it can have each network on a different subnet. (In this case, the subnet portion of the host address is the first 2 bits of the fourth, or rightmost, octet.) Another computer serves as a router connecting the two networks. It has an Ethernet card to connect to the Ethernet LAN and a Token Ring card to connect to the Token Ring. The Ethernet card is associated with or bound to the IP address 240.10.12.65. The fourth octet in this IP address is 0100 0001, which is decimal 65. The first 2 bits are the subnet address, and the remaining bits are the host address. All hosts on the Ethernet use these same subnet bits.

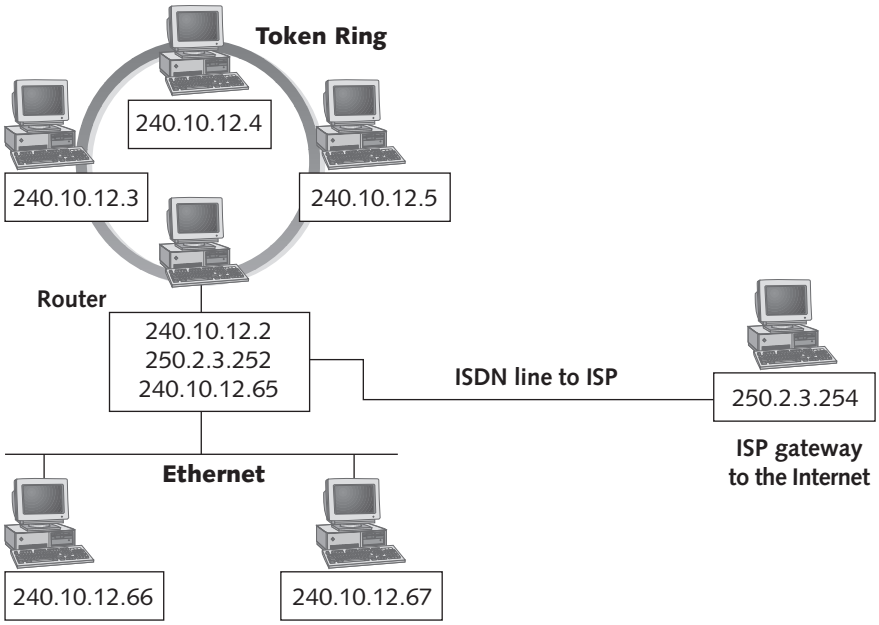


Figure 17-36 A small organization may use classless addresses with a gateway to the Internet

The router's Token Ring card is associated with an IP address of 240.10.12.2. The Token Ring network also uses a subnet mask of 255.255.255.192 for all hosts on this network. The router

has one more communication card, an ISDN card to communicate with the ISP gateway to the Internet. This ISDN card uses a third IP address, 250.2.3.252, to associate with the subnet that the gateway to the Internet is on. The router, therefore, belongs to three subnets.

A+ OS 4.2

Configuring TCP/IP with Windows 9x, Windows NT, and Windows 2000

This section contains instructions to configure TCP/IP using Windows 9x, Windows NT, and Windows 2000.

TCP/IP and Windows 9x To use TCP/IP with the networking software that comes with Windows 9x, install and configure TCP/IP under the Network window of the Control Panel. Follow these directions:

1. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Network**. Click the **Configuration** tab.
2. If TCP/IP is not already installed, click **Add** and select **Protocol** from the list of network components. Click **Add**.
3. The Select Network Protocol dialog box appears, as in Figure 17-37. Select **Microsoft** from the list of manufacturers. Select **TCP/IP** from the list of network protocols. (Notice that NetBEUI and IPX/SPX are also choices now.) Click **OK**. You will be asked to provide the Windows 9x CD-ROM or disks.

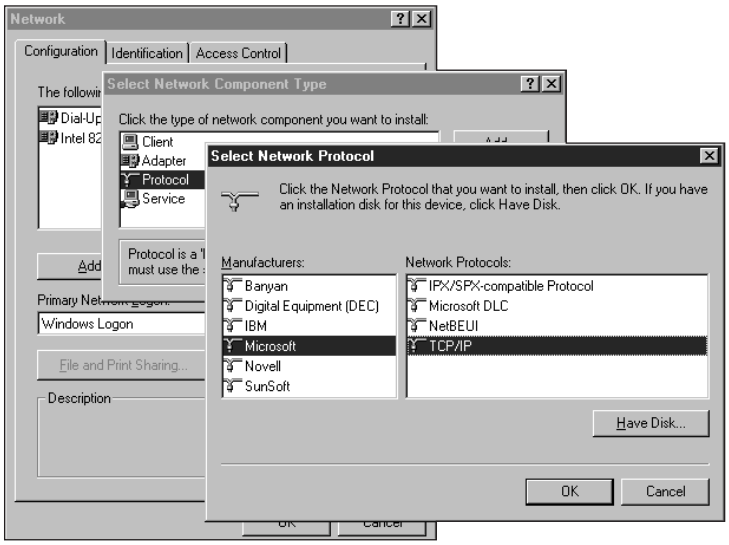


Figure 17-37 Installing TCP/IP from the Network window of the Control Panel

4. When you return to the Network window, notice that TCP/IP is automatically bound to the two adapters already installed: a network card (Intel 82595-Based Ethernet) and Windows Dial-Up Adapter (see Figure 17-38). Windows treats the

A+ OS 4.2

Dial-Up Adapter just as though it were a network card. Think of it as the software that turns your modem into a NIC.

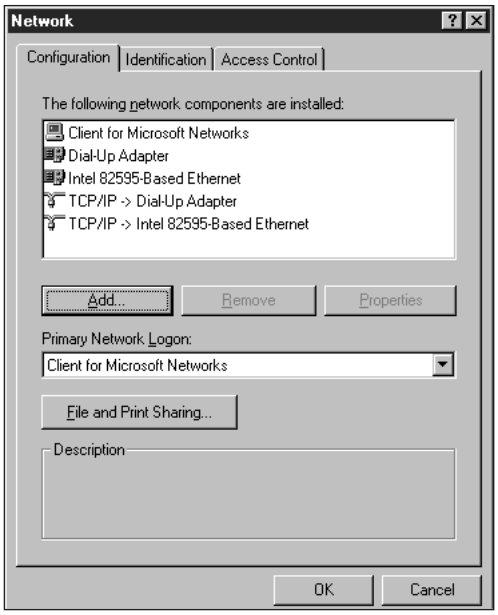


Figure 17-38 TCP/IP is automatically bound to the two network adapters already installed

5. The next step is to configure TCP/IP for each of the bindings listed that you will use. (Recall that when an IP address is associated with a network card, ISDN card, or modem, the process is called binding.) If you plan to use TCP/IP with the network card (so that the PC can communicate over networks other than its LAN), then click that selection in the list. In this case, select **TCP/IP -> Intel 82595-Based Ethernet** from the list in Figure 17-38 and then click **Properties**. The TCP/IP Properties dialog box appears, as in Figure 17-39.
6. The information in this Properties dialog box must be provided by your network administrator. For the IP Address tab, you must know if your network uses static or dynamic IP addressing. If static IP addressing is used, then click **Specify IP address** and enter the IP Address and Subnet Mask as supplied by your administrator. If dynamic IP addressing is used, click **Obtain an IP address automatically**. This will most likely be your selection when connecting to the Internet. Other tabs under this TCP/IP Properties window are discussed later in the chapter.
7. When finished, click **OK** to exit the Properties dialog box.

A+ OS 4.2

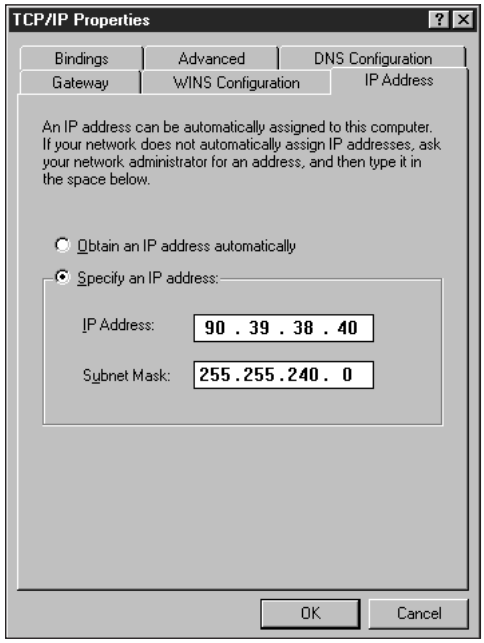


Figure 17-39 Configuring TCP/IP for static IP addressing

Using TCP/IP with Windows NT To use TCP/IP with Windows NT, first install and configure the TCP/IP protocol, and then bind it to the appropriate adapters. Follow these directions:

1. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click the **Network** icon. The Network window opens. Click the **Protocols** tab.
2. If TCP/IP is not already listed as an installed protocol, click **Add**. A list of network protocols supported by Windows NT appears, as in Figure 17-40.
3. Select **TCP/IP Protocol** and click **OK**.
4. During the installation, Windows NT asks if you plan to use a DHCP (Dynamic Host Configuration Protocol) server. If you plan to use static IP addressing, answer **No**, but if you plan to use dynamic IP addressing, as you may when connecting to the Internet, answer **Yes**.
5. You will be asked to provide the Windows NT CD-ROM and to indicate the drive and directory of the installation files. For example, for a CD-ROM drive E, enter E:\i386.
6. Click the **Close** button to close the Network window and complete the installation.
7. You can then use the TCP/IP Properties dialog box (see Figure 17-41) to configure TCP/IP for any network adapters that Windows NT detects are already installed. Again, you must choose between static and dynamic IP addressing. If you choose static, by selecting Specify an IP address, enter the IP Address, Subnet Mask, and Default Gateway for this PC. Obtain this information from your network administrator.

A+ OS 4.2

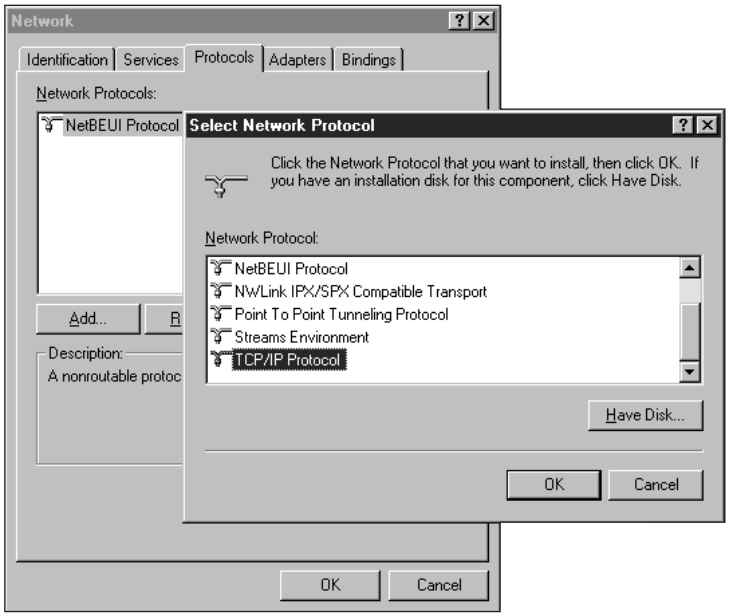


Figure 17-40 For Windows NT, install TCP/IP from the Network window of the Control Panel

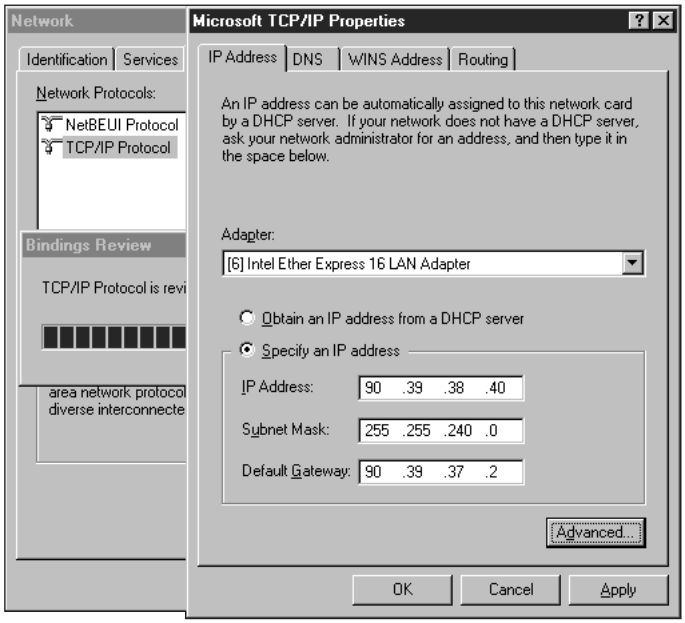


Figure 17-41 Configuring TCP/IP for Windows NT for static IP addressing

A+ OS 4.2 **Using TCP/IP with Windows 2000** TCP/IP is installed by default with most Windows 2000 installations. However, if you find it missing, follow these directions to install it, and then bind the TCP/IP properties to the NIC.

1. Using Control Panel, double-click the **Network and Dial-up Connection** icon. Right-click the connection you want to change and select **Properties** from the drop-down menu.
2. If the TCP/IP component is not listed, click **Install**. At this point, the TCP/IP installation works as it does for Windows 9x.

To set the TCP/IP properties for the connection follow the steps below.

1. Select (**Internet Protocol**) **TCP/IP** from the list of installed components and click the **Properties** button. The TCP/IP Properties dialog box opens. See Figure 17-42.
2. For dynamic IP addressing, select **Obtain an IP address automatically**. For static IP addressing, select **Use the following IP address** and enter the IP address, Subnet mask, and Default gateway.

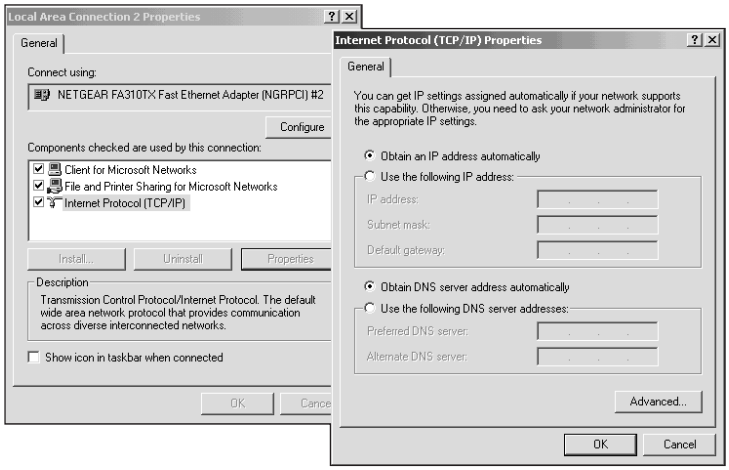


Figure 17-42 Configure a TCP/IP connection using Windows 2000

17

Connecting to the Internet

When you are supporting personal computers in a business environment where PCs are connected to a company LAN or corporate WAN, the network administrator is the final authority and is responsible for the overall support of the network. However a PC support person often is called on to help a home or small office user connect to the Internet through a dial-up connection. In this case, you are often on your own, without the help of a network administrator. You may or may not be able to call on technical support from the Internet service provider. This section looks at the process of connecting a PC running Windows 9x to the Internet, using Dial-Up Networking to make the connection.

A+ OS 4.2

Establishing Dial-up Connection to the Internet Using Windows 9x

Creating a dial-up connection to the Internet for web access and e-mail when using Windows 9x is a four-step process:

1. Install and configure your modem.
2. Configure Dial-Up Adapter.
3. Configure Dial-Up Networking.
4. Install applications software to use the Internet.

The text below describes how to do each step. Step 1 (installing and configuring a modem) is covered in Chapter 16. Once the modem is installed, follow these directions to connect to the Internet using Windows 9x:

Step 2: Configure the Dial-Up Adapter Remember that a Dial-up Adapter is Windows 9x terminology for making a modem act like a network card. The Dial-Up Adapter is automatically installed when Dial-Up Networking or Direct Cable Connection is installed. However, someone might have accidentally removed it after the installation of DUN or DCC. If necessary, you can reinstall Dial-Up Adapter from the Control Panel. Also, in Windows 95, when DUN and DCC are installed, network protocols IPX/SPX and NetBEUI are automatically installed, but not TCP/IP. Windows 98, on the other hand, automatically installs TCP/IP when DUN and DCC are installed. For Windows 98, to install TCP/IP and then bind it to the Dial-Up Adapter, follow these procedures:

1. From the **Control Panel**, open the **Network** window . If Dial-Up Adapter is not listed as an installed network component, click **Add**.
2. Select **Adapter** from the list of components to install, and then click **Add**. Manufacturers and network cards that are supported by Windows 98 are listed.
3. Select **Microsoft** as the manufacturer on the left and **Dial-Up Adapter** from the list on the right. Click **OK**. You will be asked to provide the Windows 98 CD-ROM or disks. You will then be returned to the Network window, and Dial-Up Adapter should be listed along with IPX/SPX and NetBEUI protocols.
4. To use the Internet, you need TCP/IP. Click **Add**, select **Protocol** from the list to install, and click **Add**.
5. Click **Microsoft**. From the list of supported protocols, select **TCP/IP** and click **Add**. You will be asked for the Windows 98 CD-ROM or disks.
6. After TCP/IP is installed, you are returned to the Network window. Select **TCP/IP** and then click **Properties** to configure the protocol. The Properties dialog box appears.
7. On the IP Address tab, select **Obtain an IP Address automatically**.
8. On the WINS Configuration tab, select **Disable WINS Resolution**.
9. On the Gateway tab, no installed gateways should be listed.
10. On the DNS Configuration tab, select **Disable DNS**.
11. Click **OK** to close the Properties dialog box.
12. Click **OK** to close the Network window. You might be asked to reboot the PC.

A+ OS 4.2

Step 3: Configure Dial-Up Networking If Dial-Up Networking is not installed, follow the directions earlier in the chapter to install it, then follow the directions below to create a dial-up icon for your ISP:

1. Click **Start**, point to **Programs**, **Accessories**, **Communications**, and click **Dial-Up Networking**. Double-click **Make New Connection**.
2. Verify that the modem listed under **Select a device** is the correct modem installed on your PC and enter in a name for the connection. Click **Next**.
3. Enter the phone number of your ISP and click **Finish**. The new dial-up icon appears in the Dial-Up Networking window.
4. Right-click the icon and select **Properties** from the drop-down menu. Click the **Server Types** tab (see Figure 17-43), and verify that these choices are made:
   - Type of Dial-Up Server: PPP Internet, Windows NT Server, Windows 98
   - Advanced Options: Select Enable software compression (software compression is most likely to be enabled, but this option really depends on what the ISP is doing) and Log on to network.
   - Allowed Network Protocols: TCP/IP

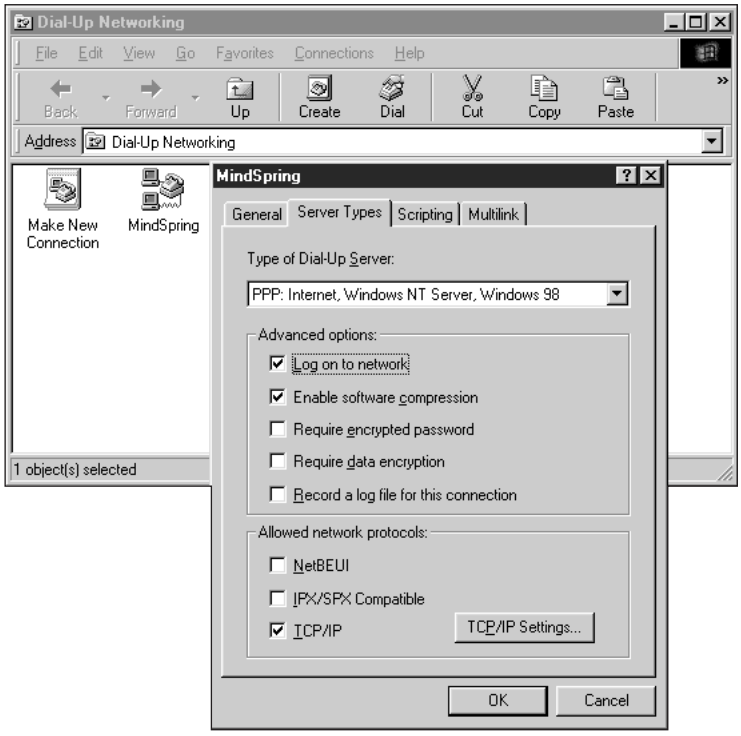


Figure 17-43 Configuring the server type for a connection to the Internet

A+ OS 4.2

5. Click **TCP/IP Settings** to open TCP/IP Settings dialog box, as in Figure 17-44. Verify that these settings are chosen:
   - Server assigned IP address
   - Specify name server addresses
   - Use IP header compression
   - Use default gateway on remote network

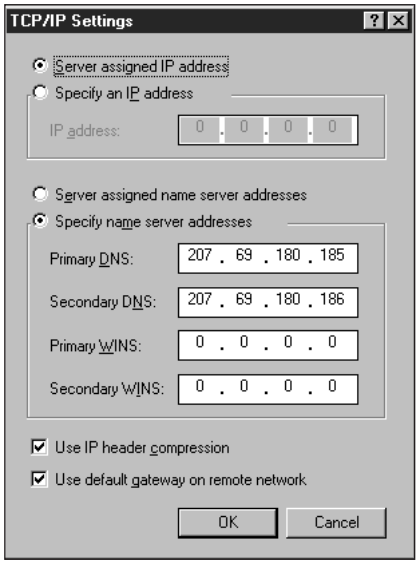


Figure 17-44 TCP/IP settings for a connection to the Internet

6. Enter the IP addresses of the Primary and Secondary DNS servers. (This information is provided by your ISP.)
7. Click **OK** two times to complete building the Dial-Up Networking connection.
8. You should now be able to dial up your ISP and see the connection complete. Once connected, however, you will not be able to use the Internet until you have installed some application-level software to access it.

Step 4: Install applications software to use the Internet

- For web browsing, install Windows 9x Internet Explorer, Netscape Navigator, or some other software provided by your ISP.
- For access to e-mail, install Windows 9x Windows Messaging (Inbox) or some other e-mail software, such as Eudora Light.

Most ISPs provide you with a web browser and e-mail software, and probably will include other software as well, such as chat room software. Install this software following the directions given to you by the ISP.

A+ OS 4.2 If you are using Internet Explorer, after you have installed the software, you can upgrade your version with the latest version of Internet Explorer from Microsoft. See directions on the company's web site, *www.microsoft.com*, to download the latest version. Internet Explorer is free to all who have a license to use a Windows OS.

There are many e-mail software programs available. A popular freeware is Eudora Light, which is likely to be included with the software from your ISP. You can download the latest version from the web site *www.eudora.com*. After you download the compressed file, execute it by double-clicking on it from Explorer. The file will decompress and a setup program executes.

Cable Modem and DSL Connections to the Internet

When connecting to the Internet using a cable modem, the service provider provides the cable modem, which is an external device that sits near your PC. The cable modem has a connection to the TV cable system of your home that connects to the ISP, and an Ethernet port to connect to your PC. An Ethernet cable connects the cable modem to a network card installed in your PC. Bind TCP/IP to this network card according to the parameters the ISP gives you.

DSL works the same way in that a device sits next to your PC, which connects to the DSL line on one side and to a network card installed in your PC on the other side. Bind TCP/IP to the network card according to the parameters the ISP gives you.

Some Examples of Network Services

At the highest level of the OSI model is the application layer, which interfaces with users and with applications software that uses networks. Figure 17-14 shows some of the more common application services: For the Internet, there are web browsers, chat rooms, e-mail, and FTP. For LANs, WANs, and corporate intranets, there are e-mail, FTP, Telnet, print services, and network drives. You have also learned from this chapter that other application-level software exists, such as middleware used to pass requests for data between a client PC and a network server. This section looks at several of the more common network services, most of which function at the top three layers of the OSI model: the application, presentation, and session layers. (Print services, an important service provided on a LAN, are covered in Chapter 18.)

Upper-Level Protocols

A+ OS 4.2 Also shown in Figure 17-14 are several upper-level protocols that function at the session and presentation layers of the OSI model, including **Hypertext Transfer Protocol** (**HTTP**) used by the World Wide Web, File Transfer Protocol (FTP) used to transfer files, and Simple Mail Transfer Protocol (SMTP) used to transfer e-mail. Sometimes these protocol names are placed in front of a computer's domain address when one computer is addressing another. The protocol, domain name, and a path or filename are collectively called a **Uniform Resource Locator (URL)**. The domain name is the only portion of a URL that is always required. An example of a URL with the three parts labeled is shown in Figure 17-45. This URL is pointing to a Web site that uses HTTP, as seen by the protocol portion of the address.

A+ OS 4.2 The path or filename portion of the URL includes a filename and file extension, document.html.

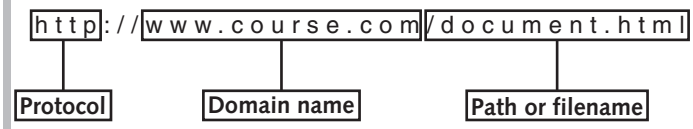


Figure 17-45 A Uniform Resource Locator (URL) can include protocol, domain name, and specific path and filename information

At the application, presentation, and session layers of the OSI model, protocols use one of two methods to establish communication with lower-level protocols: sockets or NetBIOS. Network Basic Input/Output System (NetBIOS) is mostly used on LANs for PC-based networking. It is a network extension of the older DOS BIOS used by applications software to interact with hardware. NetBEUI (NetBIOS Extended User Interface) protocol at the transport and network layers was written to interface with NetBIOS working at the session, presentation, and application layers.

Recall that a **socket** is a virtual connection (the computers are logically connected, but not necessarily physically connected) from one computer to another, such as from a PC to a server. The session-layer protocol HTTP uses the socket method to establish communication. For instance, let's look at what happens when a user requests information from a web server over the Internet. HTTP sends a request to the server to open a socket, and the socket is assigned a number for the current session. HTTP can then refer to this number when sending a GET command to the web server. The socket software then in turn uses TCP to segment and send the data. (See Figure 17-31, where the application using a socket is a web browser.) Internet protocols making connections to remote computers mostly use the socket method rather than NetBIOS. However, as you can see in Figure 17-32, the TCP/IP protocol suite includes support for NetBIOS; the protocol of TCP/IP that supports NetBIOS is NetBT.

One more concept is needed before looking at examples of network services. For all these network services, there must be a program running on both nodes of the network, for the service to work. For example, for FTP to work, FTP Client must be running at one end and FTP Server at the other. When using the World Wide Web, web browser software must be running at one end and web service software must be running on the other end. (The web service will most likely be running on a more powerful computer than a desktop PC.) Likewise, for a network drive map to work, the network drive service must be running on the host PC, and the network drive client software must be running on the client PC. Looking back at Figure 17-1, you can see this concept depicted in the diagram as the application layer on one computer logically communicating with the application layer on the other computer.

World Wide Web Browsers

Web browser software is designed to provide an interface between web sites and PCs. A web site resides on a server, has a domain name and a static IP address, and provides web pages to those computers requesting them. Using the Internet, a web browser can access a server by

A+ OS 4.2

either its IP address or its domain name. The browser can also further identify files and folders to access by putting an extension, containing paths and filenames, on the domain name. The domain name is followed by a forward slash and the path or filename to be selected.

Communication over the Web by web browsers consists of passing document files from the web server host site to the PC. The protocol used to request and pass these documents on the Web is HTTP. Often these documents are hypertext files. **Hypertext** is text that contains links or pointers to other text, files, or graphics. Hypertext is intended to be read interactively as the reader moves about over the document in a nonsequential way by selecting links either to items outside of the document or to some other point within the document. **HTML** (**Hypertext Markup Language**) is used to create hypertext and provides a way to tag links in the document. HTML documents have an .html file extension or, for DOS applications, have an .HTM file extension.

If a browser is slow, try emptying the browser cache. For Internet Explorer, click Tools, Internet Options, Delete Files, OK. You can also reduce the size of the cache to save disk space. To do that, click Tools, Internet Options, Settings, and change the size. Also, if images do not display, verify the browser setting to show pictures. To do that, click Tools, Options icon, Advanced. Under the Multimedia group check Show Pictures. The Internet Options window can also be accessed from the Control Panel.

File Transfer

A common task of communications software is file transfer, the passing of files from one computer to another. For file transfer to work, the software on both ends must be using the same protocol. The most popular way to transfer files over the Internet is with File Transfer Protocol (FTP), which is used to transfer files between two computers using the same or different operating systems. A popular use of the Internet is for companies to provide files for customers to download to their PCs, such as when new upgrades for software become available. This service is commonly provided by Windows 2000, Windows NT or UNIX servers that provide access to files using FTP and are called **FTP servers** or **FTP sites**. These commercial FTP sites only provide the ability to download a file to your PC. However, FTP offers more power than just that. A user who has first logged on to a remote computer can use FTP utility software to copy, delete, and rename files, make directories, remove directories, and view details about files and directories.

Most communications applications provide a file transfer utility that has its own look and feel, but the basics of file transfer are the same from one utility to another. The text below discusses a couple of examples of file transfer utilities, highlighting their similarities and differences.

File Transfer from a Command Prompt

FTP can be initiated at a DOS, Windows 9x, Windows NT, or Windows 2000 command prompt, if a connection is established to a network or the Internet. Operating FTP from a command prompt is a quick-and-dirty way to transfer files when the computer does not have more user-friendly FTP software installed. For example, Windows NT Workstation has FTP available at the command prompt, but a GUI version of FTP is not packaged with the OS and must be installed. The FTP DOS commands work like the dialog in Table 17-5.

A+ OS 4.2

Table 17-5 A sample FTP session from a DOS command prompt

Command Entered at the DOS Command Prompt	Description
FTP	Execute the DOS FTP utility
OPEN 110.87.170.34	Open a session with a remote computer having the given IP address
LOGIN: XXXXXX	The host computer provides a prompt to enter a user ID for the computer being accessed.
PASSWORD: XXXXXX	The host computer requests the password for that ID. Logon is then completed by the host computer.
CD /DATA	Change directory to the /DATA directory
GET YOURFILE.DAT	Copy the file YOURFILE.DAT (or whatever file you want) from the remote computer to my computer
PUT MYFILE.DAT	Copy the file MYFILE.DAT (or whatever file you want) from your computer to the remote computer
BYE	Disconnect the FTP session

File Transfer Using FTP Software

FTP client software can be downloaded from the Internet or directly from your ISP. This example looks at how to execute FTP using such software:

1. Start the FTP utility software. The FTP utility screen appears similar to the one in Figure 17-46.
2. Click **Connect** to log on to an FTP site. A Session Profile dialog box appears, such as the one in Figure 17-46.
3. Enter the Host Name, for example ftp.course.com. Enter the User ID and Password for this host computer, and then click **OK**.
4. The connection is made, and your ID and password are passed to the host. After you have been authenticated by the host computer, a screen similar to that in Figure 17-47 is displayed.
5. The files on the left belong to you, and the files on the right belong to the remote host computer. You can drag and drop files either to or from the other computer, or you can use the commands at the bottom of the window. Notice in Figure 17-47 the choices toward the bottom of the window: ASCII, Binary, or Auto. These choices refer to the format that is to be used to transfer the files. Use ASCII only for text files, and use Binary for all others. If you are not sure which to use, choose **Auto**.
6. When transferring files is complete, click **Exit** to leave the utility.

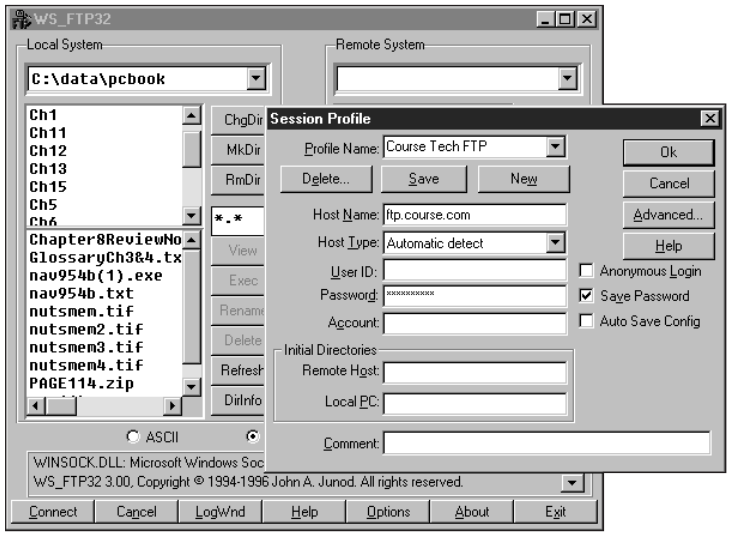


Figure 17-46 A typical FTP utility provided by an Internet service provider

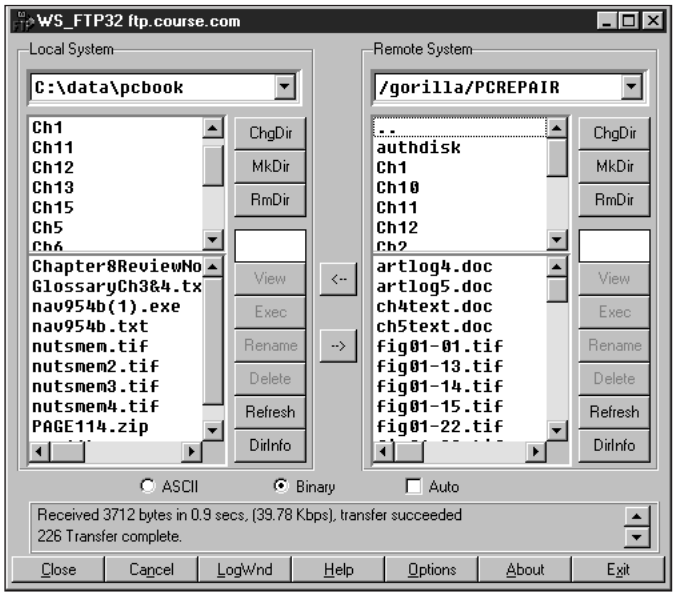


Figure 17-47 An FTP utility screen showing local and remote files

Many web pages provide the ability to download a file. It is likely that this file is not being downloaded from the web server, but the author of the web page has programmed a link from the web page to an FTP server. When you click the filename on the web page, the program controlling the page executes FTP commands to the FTP server to download the file to you. If you receive an error, you can sometimes solve the problem by going directly to the

company's FTP server and using an FTP utility (such as the one described here) to download the file or even see a list of other files that you might also like to download.

Network Drive Map

A+ OS 4.1

A network drive map is one of the most powerful and versatile methods of communicating over a network. By using network file service (NFS) software, the network drive map makes one PC appear to have a new hard drive, such as drive E, that is really hard drive space on another host computer. Even if the host computer is using a different OS, such as UNIX, the drive map still functions. Using a network drive map, files and folders on a host computer are available even to network-unaware DOS applications. The path to a file simply uses the remote drive letter instead of a local drive such as drive A or drive C.

The following example connects two computers, using Dial-Up Networking. The host computer is using Windows NT, and the local computer is using Windows 95 (although Windows 98 works just the same way). The Windows 95 PC will map a network drive to the Windows NT PC.

Preparing a Windows NT Host Computer for a Network Drive Map

For Windows NT to allow a remote PC to dial in, Remote Access Service (RAS) must be installed and running. The remote user must have been set up with a user ID and password, and drives and/or folders must be shared, meaning that other computers are allowed to have access to them.

Follow these directions for setting up a Windows NT PC to allow a remote PC to map a network drive using Windows 95:

1. To install RAS, click **Start**, point to **Settings**, click **Control Panel**, and then double-click the **Network** icon.
2. Select the **Services** tab. If Remote Access Service is not already listed as being installed, click **Add**. From the list of Network services, select **Remote Access Service** and click **OK** to install the service. You will be asked to supply the Windows NT CD-ROM and the path to the \i386 directory on the CD.
3. From the Network window, select **Remote Access Service** and click **Properties**. The Remote Access Setup dialog box appears, as in Figure 17-48.
4. Click **Configure**. The Configure Port Usage dialog box appears, as in Figure 17-49. Select **Dial out and Receive calls**. Click **OK**.

A+ OS 4.1

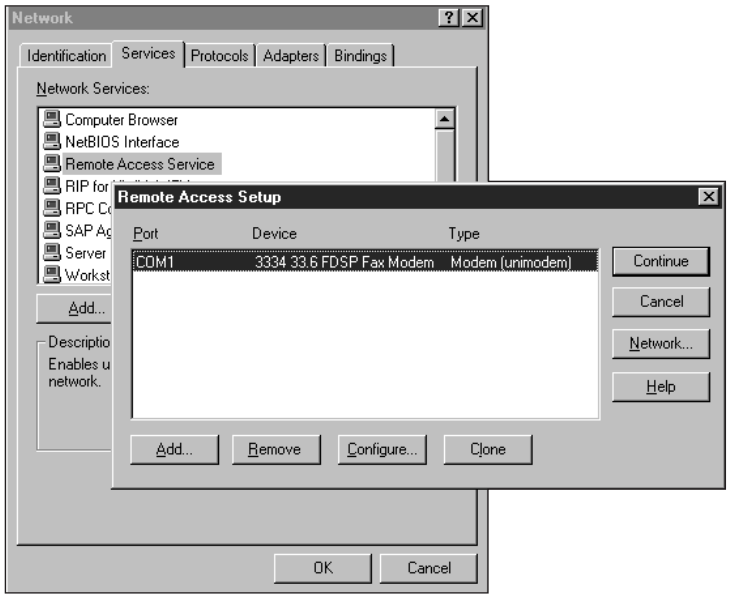


Figure 17-48 Remote Access Service allows another PC to dial in to a Windows NT PC

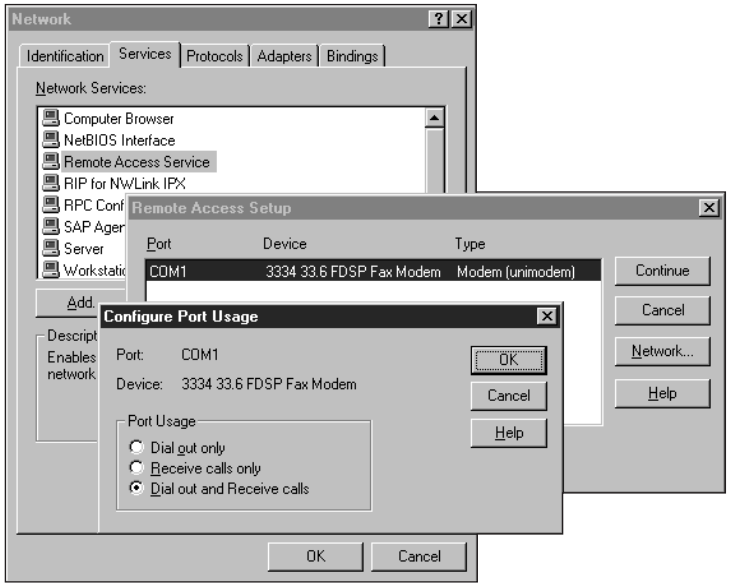


Figure 17-49 Configuring RAS under Windows NT to allow both incoming and dial-out calls

5. From the Remote Access Setup dialog box, click **Network**. The dialog box shown in Figure 17-50 appears, including the three network protocols for dial-out or dial-in calls. For one PC to connect to another, NetBEUI is the most efficient

A+ OS 4.1

choice. You can select only NetBEUI or leave others selected as well. For a Novell LAN, use IPX, and use TCP/IP to connect to the Internet. Click **OK** and then **Continue** to return to the Control Panel.

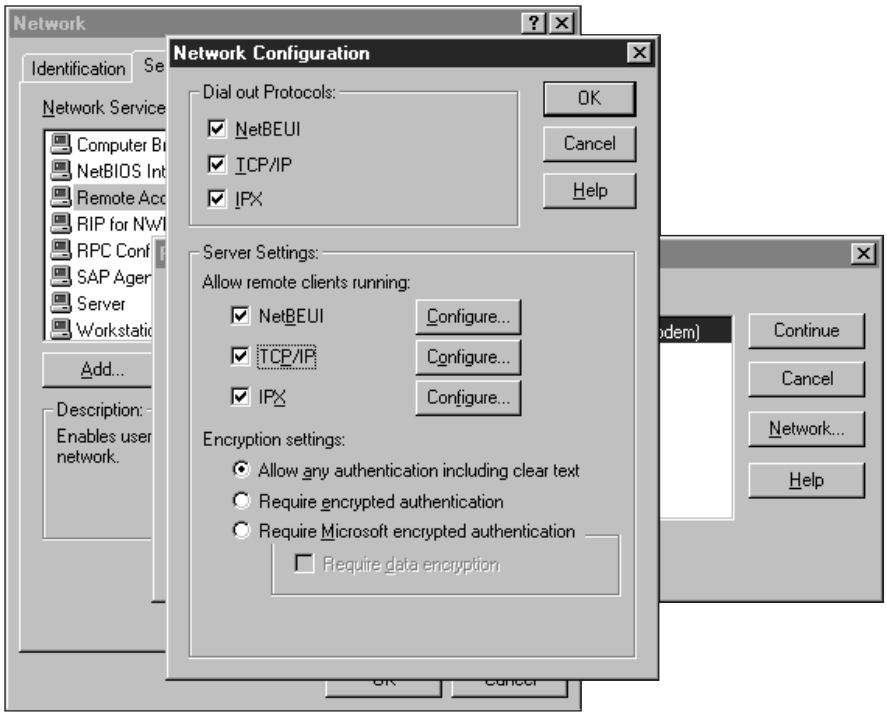


Figure 17-50 Windows NT RAS supports three network protocols

6. Once RAS is installed, it can be set to start automatically each time you boot, or you can start it manually. To start the RAS service, click **Start**, point to **Settings**, click **Control Panel**, and double-click **Services**. Select **Remote Access Server** and then click **Start**.
7. Follow instructions from Chapter 13 to set up a user ID and password from the User Manager. (Click **Start**, point to **Programs**, **Administrative Tools**, and click **User Manager**.) Be sure to grant the user the permission to dial in from a remote PC.
8. To establish which drives and/or folders you want the remote user to access, open Explorer, and then right-click the drive or folder you want to share. Select **Sharing** from the drop-down menu. Select **Shared As** and give the resource a name, such as MarketFolder or C. The workstation is now set to allow a dial-in. The next time you want to allow the remote use of the PC, all that you must do is start RAS.

A+ OS 4.1

Mapping the Network Drive from a Remote to a Host Computer

To set up a host computer and to allow a network drive to map to your hard drive, or to access the network drive from a remote computer, each computer must be running network drive software. Windows NT and Windows 9x include support to map network drives to other Windows PCs. To map network drives to computers using other OSs, you must use third-party software.

The remote computer can use either a regular network connection or Dial-Up Networking to connect to the host computer. After you are connected, to map a network drive on your computer, use Windows Explorer. Follow these directions:

1. While connected to a network, access Windows Explorer. Click the **Tools** menu shown in Figure 17-51. Select **Map Network Drive**.

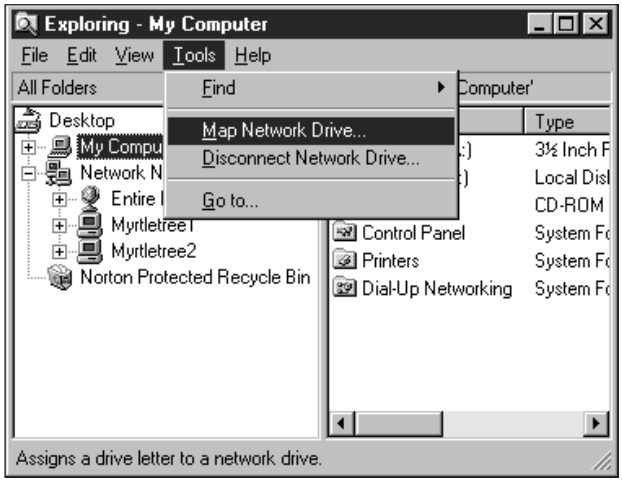


Figure 17-51 Mapping a network drive to a remote computer, using Windows Explorer

2. The Map Network Drive dialog box appears, as in Figure 17-52. Select a drive letter from the drop-down list.
3. Enter a path to the host computer. Use two backslashes, followed by the name of the host computer, followed by a backslash and the drive or folder to access on the host computer. For example, to access drive C on the computer named MyrtleTree1, enter **\\MYRTLETREE1\C** and then click **OK**.
4. Figure 17-53 shows the results of the drive map. There is a new drive E displayed in Windows Explorer. Folders listed on the right side of the figure are on the host PC.

A+ OS 4.1

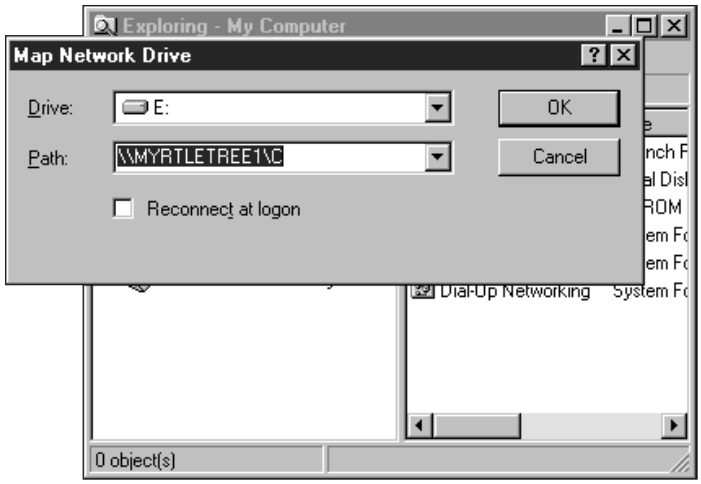


Figure 17-52 To map a network drive, enter a drive letter to use on your PC and the path to the remote computer

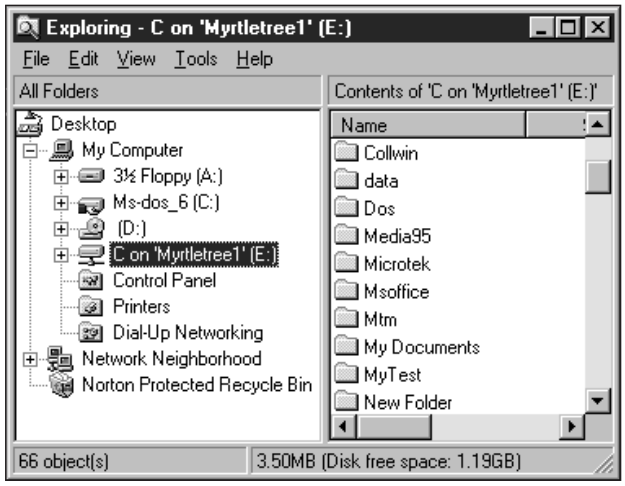


Figure 17-53 Folders listed on the right side of Windows Explorer belong to the remote computer. This computer sees them belonging to its drive E.

Linux Operating System

Network services often are provided by a computer running the Linux operating system. Linux is well-suited to support web servers, FTP servers, and file servers. Because Linux is very reliable and does not require a lot of computing power, it is sometimes used as a desktop OS, although it is not as popular for this purpose because it is not easy to use. As a PC support technician, you should know a little about Linux, including a few basic commands.

Recall from earlier chapters that an operating system is composed of a kernel, which interacts with the hardware and other software, and a shell, which interacts with the user and the kernel. Linux is a UNIX-like operating system, and, just as with other versions of UNIX, can use more than one shell. The default shell for Linux is the Bash shell. The name stands for "Bourne Again Shell" and takes the best features from two previous shells, the Bourne and the Korn shells.

The system administrator is responsible for a Linux or UNIX server. This person installs updates to the OS (called patches), manages backup processes, supports the installation of software and hardware, sets up user accounts, resets passwords, and generally supports users. The system administrator has root privileges, which means that he or she can access all the functions of the OS and the principal user account called the root account. The administrator protects the password to the root account because this password gives full access to the system. When the administrator is logged on, he or she is logged on as the user root. For example, you can use the who command to show a list of all users currently logged on to the system. Type **who** to see that three users are currently logged on: the root, james, and susan.

```
who
root        tty1        Oct 12 07:56
james       tty1        Oct 12 08:35
susan       tty1        Oct 12 10:05
```

The command prompt for the root is different from the command prompt for ordinary users. The root command prompt is # and other users have the $ command prompt.

The main directory in UNIX is the root directory and is written with a forward slash. For example, use the ls command, which is similar to the DOS DIR command, to list the contents of the root directory. The command (ls -l /) and its results are shown in Figure 17-54. Notice that the -l parameter is added to the command, which displays the results using the long format. Also notice in the figure the format used to display the directory contents. The d at the beginning of each entry indicates that the entry is a directory, not a file. The other letters in this first column have to do with the read and write privileges assigned to the directory and the right to execute programs in the directory. The name of the directory is in the last column. The rights assigned the directory can apply to the owner of the directory, other users, or to an entire group of users.

UNIX Commands

This section describes some basic UNIX commands together with simple examples of their use. As you read along, know that all commands entered in Linux or UNIX are case sensitive.

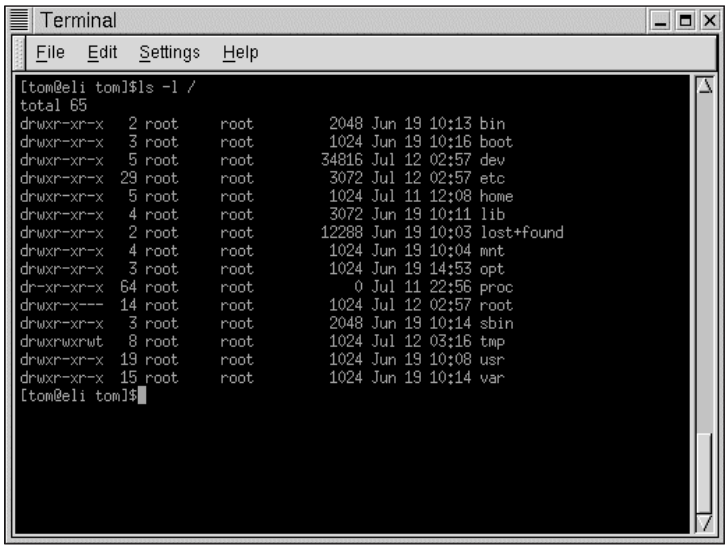


Figure 17-54 Use the ls command to display directory contents

Table 17-6 Some common UNIX commands

Command	Description
echo	Displays information on the screen. For example, to display which shell is currently being used, enter this command: `echo $SHELL`
clear	Clears the screen
man	Displays the online help manual called the man pages. For example, to get information about the echo command: `man echo` The manual program displays information about the command. To exit the manual program, `type q`.
whatis	Use the whatis command to display a brief overview of a command. For example, to get quick information about the echo command: `whatis who`

cat	The cat command lets you view the contents of a file. For example, to display a file:
	`cat /etc/shells`
	This command displays the contents of the file named shells which is located in the /etc directory. Use the forward slash when giving the path to a file rather than the back slash used by Windows.
	Many UNIX commands can use the redirection symbol > to redirect the output of the command. For example, use the redirection symbol with the cat command to copy a file:
	`cat /etc/shells > newfile`
	The contents of the shells file is written to newfile.

Table 17-6 Some common UNIX commands (continued)

Command	Description
cd	Change directory. For example, `cd /etc` changes the directory to /etc.
ls	The ls command is similar to the DOS DIR command. For example, to list all files in the /etc directory, using the long parameter for a complete listing: `ls -l /etc`
chmod	This command changes the attributes assigned to a file and is similar to the DOS ATTRIB command. For example, to grant read permission to the file myfile: `Chmod +r myfile`

Managing Processes

If the Linux system is a web or e-mail server, then the web or e-mail server application runs as a process in the background. When a process runs in the background, no information is displayed on the screen about that process. When you initiate a process to run in the background, enter the name of the process at the command prompt followed by the &. For example, to run the program myserver in the background, enter this command:

```
$ myserver &
862
```

Linux starts the process and responds with a number, which is the process identifying number (PID). This number can be different each time the process is started. You can use this PID to later stop the process.

To get a listing of all currently running processes together with their PIDs, use the ps command like this:

```
$ ps
PID        TTY        TIME        CMD
648        pts/0      00:00:00    bash
709        pts/0      00:00:00    ps
862        pts/0      00:00:00    myserver
```

To stop a process, use the kill command. To kill a process, you can refer to the process name or the PID. If the process name is used in the kill command, precede the name with the %. For example, to kill the process myserver, use either command:

```
kill 862
kill %myserver
```

Windows Managers

Because many users prefer a Windows desktop, several applications have been written to provide a GUI shell for UNIX and Linux. These shells are called X Windows. A typical X Window screen is shown in Figure 17-55. One popular desktop environment software that runs on top of a windows manager is GNU Network Object Model Environment (GNOME). GNOME (pronounced "guh-nome") provides a desktop that looks and feels

like Windows 98, and is free software designed to use a Linux kernel. The major components of a GNOME window are showing in Figure 17-56. For more information about GNOME, see the organization's web site at *www.gnu.org*.

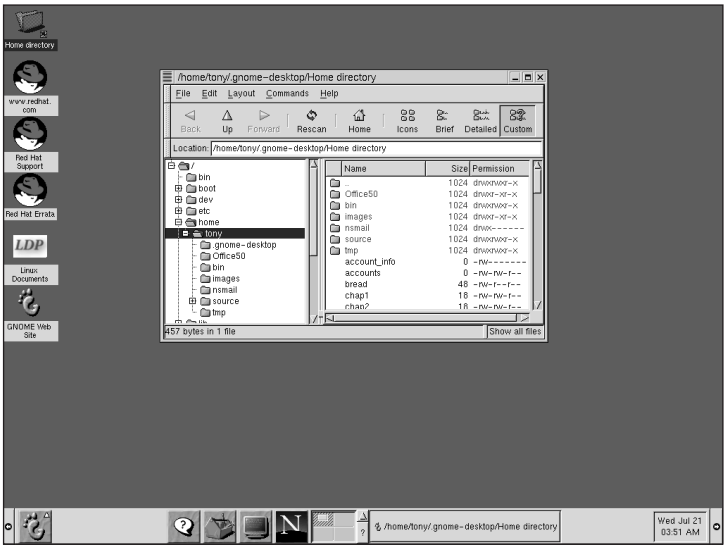


Figure 17-55 X Windows software provides a GUI shell for Linux and UNIX users

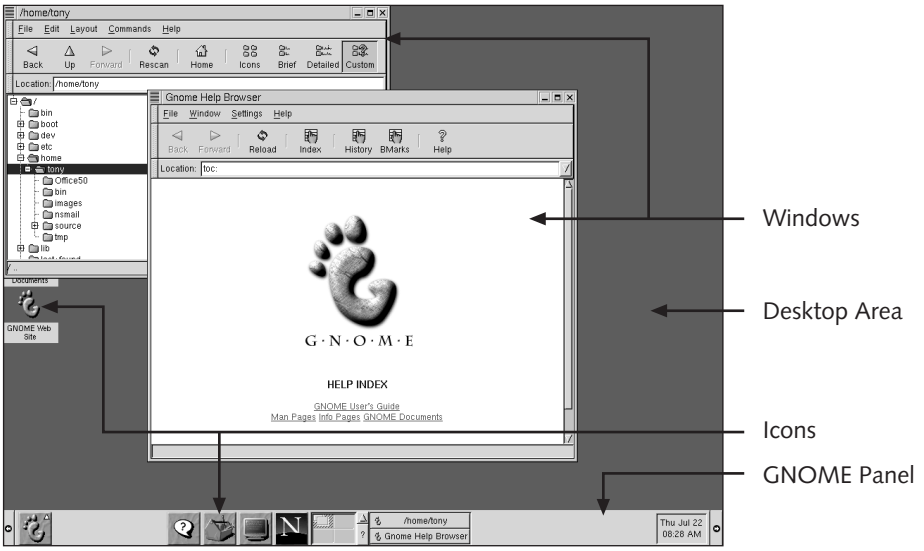


Figure 17-56 GNOME is popular desktop environment software used on Linux systems

NETWORK TROUBLESHOOTING GUIDELINES

This section covers some guidelines to use when troubleshooting network problems.

Windows 9x Dial-Up Problems

A+ OS 3.2, 4.2

Below are Windows 9x dial-up problems you will face and suggestions for solving them.

Modem problems

Problems that arise when dialing into a host computer using Windows 95 Dial-Up Networking may be caused by the modem. See Chapter 16 for troubleshooting guidelines for modems.

Cannot make a connection Sometimes a computer cannot connect to the network. Because Dial-Up Networking involves so many different components, first find out what works and what doesn't work. Find out the answers to these questions:

- Does the modem work? Compare the printout of a Modemlog.txt file that was made during a successful connection at another PC to the Modemlog.txt file of this PC, to identify the point in the connection at which an error occurs. (For Windows 9x, to log modem events to the Modemlog.txt file, double-click **Modems** in Control Panel, then select the modem, click **Properties**, **Connection**, **Advanced**, and turn on **Recording to a log file**.)
- Are all components installed? Check for the Dial-Up Adapter and TCP/IP, and check the configuration of each.
- Check the Dial-Up Networking connection icon for errors. Is the phone number correct? Does the number need to include a 9 to get an outside line? Has a 1 been added in front of the number by mistake?
- Reboot your PC and try again.
- Try removing and reinstalling each network component. Begin with TCP/IP.
- Try dialing the number manually from a phone. Do you hear beeps on the other end?
- Try another phone number.
- Sometimes older copies of the Windows socket DLL may be interfering with the current Windows 9x socket DLL. (Windows 9x may be finding and executing the older DLL before it finds the newer one.) Search for and rename any files named Winsock.dll except the one in the Windows\System directory.

A+ OS 3.2, 4.2

You can connect, but you get the message "Unable to resolve hostname..." This error message means that TCP/IP is not able to determine how to route a request to a host. Right-click the **Dial-Up Networking** connection icon, select **Properties**, and check for these things:

- Under Server Type, try making TCP/IP the only network protocol allowed.
- Under TCP/IP settings, check the IP addresses of the DNS servers.
- Make sure **Using the default gateway** is selected.
- Try *not* selecting IP header compression.

After connecting, you get the error message "Unable to establish a compatible set of network protocols" This error is most likely to be caused by a problem with the installation and configuration of Dial-Up Networking and/or TCP/IP. Try these things:

- Verify that Dial-Up Adapter and TCP/IP are installed and configured correctly.
- Remove and reinstall TCP/IP. Be sure to reboot after the installation.
- Try putting the Windows 9x PCs in different workgroups.
- Windows 9x can write the events of PPP processing a call to a log file. Create the Ppplog.txt file on a PC that makes a successful connection, and compare it to the log file of your bad connection to see exactly when the problem began. To turn on the logging of events to the file, double-click the **Network** icon in Control Panel. Click **Dial-Up Adapter**, click **Properties**, select the **Advanced** tab and select **Record a log file**. On the Value list, click **Yes**, then click **OK**. Reboot the PC. The file Ppplog.txt is created in the Windows folder as the connection is made and used.

When you double-click the network browser, the modem does not dial automatically. When this occurs, right-click the network browser icon and select **Properties** from the drop-down menu. Under the Connection tab, check **Connect to the Internet as needed**.

Problems with TCP/IP

Windows 9x and Windows NT offer several utilities that can help in troubleshooting TCP/IP. Some are introduced here.

Problems with TCP/IP Configuration or Suspected Network Problems

A useful diagnostic tool for either Windows 9x or Windows NT is **Packet Internet Groper** (**PING**), which tests connectivity. PING sends a signal to a remote computer. If the remote computer is online and hears the signal, it will respond. Ipconfig under Windows NT and Windows 2000 and Winipcfg under Windows 9x test TCP/IP configuration. Try these things:

- For Windows NT, at the command prompt, enter **Ipconfig**, or, for Windows 9x, click **Start**, **Run** and enter **WinIPcfg** in the Run dialog box and click **OK**. If the TCP/IP configuration is correct, for static IP addressing, the IP address, subnet

A+ OS 3.2, 4.2

mask, and default gateway appear along with the adapter address. If DHCP is used for dynamic IP addressing and no IP address has yet been assigned, the IP address should read 0.0.0.0.

- Try to release the IP address and request a new one, which might reestablish a connection. On the WinIPcfg window, select the network adapter and click Release and Renew.
- Next try the loopback address test. Enter the command PING 127.0.0.1. This IP address refers to you. It should respond with a reply message from you. If this works, TCP/IP is likely to be configured correctly.
- If you have been assigned an IP address, PING it. If you get any errors up to this point, then assume that the problem is on your PC. Check the installation and configuration of each component. Remove and reinstall each component and watch for error messages. Compare the configuration to that of a PC that is working on the same network.
- Next PING the IP address of your default gateway. If it does not respond, then the problem may be with the gateway or with the network to the gateway.
- Now try to PING the host computer you are trying to reach. If it does not respond, then the problem may be with the host computer or with the network to the computer.
- If you substitute a URL for the IP address in the PING command, and the PING works, then you can conclude that DNS works. If an IP address works, but the URL does not work, the problem lies with DNS. Try this: PING *microsoft.com*.
- Use Tracert to trace the route to the remote computer: Try tracert microsoft.com or substitute an IP address in the command line.
- Under Windows 2000, to resolve a problem with DNS, use Nslookup to display information about a domain name kept on a DNS server. Try Nslookup microsoft.com

CHAPTER SUMMARY

- A network can be either a LAN or a WAN. Connecting LANs and WANs together is called internetworking.
- The three most popular network technologies today are Ethernet, Token Ring, and FDDI. Each is designed to satisfy a different networking need. ATM is a relatively new network technology that is faster than the other three.
- Ethernet can follow either a bus or star physical design and is the least expensive and most popular network type. Token Ring is more reliable, but more expensive and difficult to maintain. FDDI is used to fill massive networking needs over a wide area, for example, serving as the backbone network between smaller networks in a large building complex such as a large hospital.
- There are several kinds and grades of networking cables, including coaxial cable, unshielded twisted-pair (UTP) cable, shielded twisted-pair (STP) cable, and fiber-optic cable.
- Segmentation is a method of breaking a large network into smaller segments in order to control traffic over the network.

- Bridges, routers, switches, and gateways are used to interconnect networks.
- Repeaters are used to amplify signals that are traveling a long distance on a network.
- A network interface card (NIC) prepares data for transmission by disassembling the data into data segments and encapsulating the packet with header and trailer information. It then transmits the data packet over cabling media, and reassembles the data back into a contiguous stream at the receiving end.
- Each NIC has embedded on it at the factory a unique identifying 6-byte hex number called the media access control (MAC), or adapter, address. This number uniquely identifies the NIC on the network and physically identifies the node on the network.
- The seven-layer OSI network model is used as a guideline for discussing the different protocols, software, and firmware of a network. Mapping the many different components onto the model helps in understanding how they interrelate and what function each serves for the network.
- Examples of networking software components that satisfy the bottom two layers of the OSI model (physical and data-link layers) are Ethernet, Token Ring, FDDI, and PPP over phone lines. Examples of protocols that work at the network, transport, and session layers are TCP/IP, IPX/SPX, and NetBEUI. Software examples of the top OSI layers (presentation and application) are web browsers, e-mail and chat room software, and Telnet.
- Windows 9x, Windows NT, and Windows 2000 support phone line access to networks. This OS service is called Dial-Up Networking, and it makes a modem appear to be a NIC on the network.
- Windows 9x, Windows NT, and Windows 2000 also support direct cable connection, a method of networking two PCs with a serial or parallel cable.
- The Internet is a huge interconnection of many networks. It provides a decentralized way to successfully route data over many networks that use varying protocols, software, and hardware. The principal protocol of the Internet is TCP/IP, which identifies each node on the network with an IP address that ultimately must match up with the computer's MAC address.
- An IP address has two parts: a network address identifying the network, and a host address identifying the individual PC on the network. Sometimes the network address also includes a subnet address to allow a network to be broken up into logical segments in order to control traffic within the network.
- IP addresses can be permanently assigned to PCs (called static IP addressing) or dynamically assigned. When IP addresses are dynamically assigned, a different IP address is assigned to a host each time the host goes online to the network. Servers that manage dynamic assignments of IP addresses are called DHCP (Dynamic Host Configuration Protocol) servers.
- A domain name is a convenient and user-friendly method of naming a host on a network. A domain name must ultimately be mapped to the IP address of the host before data can be routed to the host. Two services that track domain names and their corre-

sponding IP addresses are DNS (Domain Name Service) and WINS (Windows Internet Naming Service).

- TCP/IP is really a suite of protocols that satisfy differing needs of a network and include the network, transport, and session layers of the OSI model.
- Once connection to the Internet is made using TCP/IP and PPP (with a modem), software at the higher layers of the OSI model is used to send and receive data over the network. Different types of Internet software access different Internet services, including web browsing, e-mail, and FTP.
- Important networking services typically used on smaller networks are network drive maps and print services.

KEY TERMS

Adapter address — A 6-byte hex hardware address unique to each NIC and assigned by manufacturers. The address is often printed on the adapter. An example is 00 00 0C 08 2F 35. Also called MAC address.

Address Resolution Protocol (ARP) — A method used by TCP/IP that dynamically or automatically translates IP addresses into physical network addresses such as Ethernet IDs or Token Ring MAC addresses.

Alternate gateway — An alternate router that is used if the default gateway is down. *See* Gateway.

Amplifying repeater — A repeater used on a broadband network that amplifies whatever it receives regardless of its source.

Application layer — The layer of the OSI model responsible for interfacing with the user or application using the network.

Back end — In a client/server environment, the application on the server that processes requests for data from the client.

Backbone — A network used to link several networks together. For example, several Token Ring and Ethernet LANs may be connected using a single FDDI backbone.

Baseband — Relating to a communications system which carries only a single message at a time over wire. Ethernet uses baseband technology. Compare to broadband.

Binding — Associating an OSI layer to a layer above it or below it. For example, associating a protocol type such as TCP/IP to a NIC driver.

BNC connector — A connector used on an Ethernet 10Base2 (Thinnet) network. A BNC connector looks like a TV cable connector.

Bridge — A hardware device or box, coupled with software at the data-link layer, used to connect similar networks and network segments. A bridge uses a MAC address to determine which network gets a packet.

Broadband — Relating to a communications system such as cable modem or ATM networks that carry multiple messages over wire, each message traveling on its own frequency. Compare to baseband.

Bus network topology — A network design in which nodes are connected in line with one another, with no centralized point of contact.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) — A feature used in Ethernet networks whereby packets are sent after the sending node listens for silence, and are resent if a collision is detected.

Classless addresses — Class C network addresses that are used in subnets where the subnet masks don't fall on full octets

Collision — In an Ethernet network, a collision occurs when transmitted packets of data are sent at the same time and collide. Ethernet will first listen for silence before it transmits, and it will stop and resend if a collision occurs.

Combo card — An Ethernet card that has more than one port to accommodate different cabling media.

Connection protocol — In networking, confirming that a good connection is made before transmitting data to the other end. To accomplish this, most network applications use TCP rather than UDP.

Connectionless protocol — When UDP is used and a connection is not required before sending a packet. Consequently, there is no guarantee that the packet will arrive at its destination. An example of a UDP transmission is a broadcast to all nodes on a network.

Contention-based system — A system in which each computer contends for the opportunity to transmit on the network. If there is a collision, a computer waits a random amount of time and resends.

Controlled-access unit (CAU) — A centralized hub on a Token Ring network. *See* Multistation access unit.

Crosstalk — The interference that one wire, in a twisted pair, may produce in the other.

Data-link layer — The OSI layer that disassembles packets and reassembles data into packets.

Default gateway — The main gateway or unit that will send or receive packets addressed to other networks.

Dial-Up Networking (DUN) — A Windows application that allows a PC to remotely connect to a network through a phone line. A Dial-Up Network icon can be found under My Computer.

Domain name — A unique, text-based name that identifies an IP (Internet address). Typically, domain names in the United States end in .edu, .gov, .com, .org, or .net. Domain names also include a country code, such as .uk for the United Kingdom.

Domain Name System or **Domain Name Service (DNS)** — A database on a top-level domain name server that keeps track of assigned domain names and their corresponding IP addresses.

Dynamic Host Configuration Protocol (DHCP) — The protocol of a server that manages dynamically assigned IP addresses. DHCP is supported by Windows 9x, Windows NT, and Windows 2000.

Dynamic IP address — An assigned IP address that is used for the current session only. When the session is terminated, the IP address is returned to the list of available addresses.

Ethernet — The most popular network topology used today. It uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and can be physically configured as a bus or star network.

FDDI (Fiber Distributed Data Interface) — Pronounced "fiddy." A ring-based network, similar to Token Ring, that does not require a centralized hub. FDDI often uses fiber-optic cabling.

Frame — The header or trailer information added to data to encapsulate it before it is sent over a network.

Front end — In a client/server environment, the application on the client that makes use of data stored on the server.

FTP (File Transfer Protocol) — An Internet standard that provides for the transfer of files from one computer to another. FTP can be used at a command prompt, or with a GUI interface, which is available with FTP software or with a web browser. When using a web browser, enter the command "ftp" in the browser URL line instead of the usual "http://" used to locate a web site.

FTP server or **FTP site** — A computer that stores files that can be downloaded by FTP.

Gateway — A device or process that translates protocol types between networks.

Header — Information sent ahead of data being transferred over a network to identify it to receiving protocols. An IP header consists of items such as header and data packet length, flags, checksum, addresses, and so on.

Hop count — The number of routers a packet must pass through in a network in order to reach its destination.

HTML (Hypertext Markup Language) — The language used to create hypertext documents commonly used on web sites. HTML documents have an .html file extension.

HTTP (Hypertext Transfer Protocol) — The common transfer protocol used by Internet browsers on the World Wide Web.

Hub — A network device or box that provides a central location to connect cables.

Hypertext — Text that contains links to remote points in the document or to other files, documents, or graphics. Hypertext is created using HTML and is commonly distributed from web sites.

Intelligent hubs — Network hubs that can be remotely controlled at a console, using network software. These hubs can monitor a network and report errors or problems.

Internet — The worldwide collection of over a million hosts that can communicate with each other using TCP/IP. The lowercase *internet* simply means multiple networks connected together.

Internet Control Message Protocol (ICMP) — Part of the IP layer that is used to transmit error messages and other control messages to hosts and routers.

Internet service provider (ISP) — A commercial group that provides a user with Internet access for a monthly fee. AOL, Prodigy, GTE, and CompuServe are four large ISPs.

Internetwork — Two or more networks connected together, such as a LAN and a WAN joined together.

Intranet — A private internet used by a large company.

IP (Internet Protocol) address — A 32-bit "dotted-decimal" address consisting of four numbers separated by periods, used to uniquely identify a device on a network that uses TCP/IP protocols. The first numbers identify the network; the last numbers identify a host. An example of an IP address is 206.96.103.114.

IPX/SPX — A protocol developed and used by Novell NetWare for LANs. The IPX portion of the protocol works at the network layer, which is responsible for routing, and the SPX portion of the protocol manages error checking at the transport layer.

Limited token — Applies to a FDDI network. A token sent that allows a receiving station to communicate only with the sending station, thus providing continuous communication between the two stations.

Line protocol — A protocol used over phone lines to allow a connection to a network. Also called a bridging protocol. The most popular line protocol is PPP (Point-to-Point Protocol).

MAC (media access control) — An element of data-link layer protocol that provides compatibility with the NIC used by the physical layer. A network card address is often called a MAC address. *See* Adapter address.

Middleware — Software necessary for an application on a client to pass requests to a server, and for a server to respond with data. Microsoft's Open Database Connectivity (ODBC) is an example of middleware.

Multiframe dialog — When a limited token is sent that allows a receiving station to communicate only with the sending station, thus providing continuous communication between the two stations.

Multistation access unit (MSAU or **MAU)** — A centralized device used to connect IBM Token Ring network stations.

Nearest active downstream neighbor (NADN) — The next station to receive a token in a token ring.

Nearest active upstream neighbor (NAUN) — The station that has just sent a token to the nearest active downstream neighbor in a token ring.

NetBEUI (NetBIOS Extended User Interface) — A proprietary Microsoft networking protocol used only by Windows-based systems, and limited to LANs because it does not support routing.

NetBT (NetBIOS over TCP/IP) — An alternate Microsoft NetBEUI component designed to interface with TCP/IP networks.

Network interface card (NIC) — A network adapter board that plugs into a computer's system board and provides a port on the back of the card to connect a PC to a network.

Network layer — The OSI layer responsible for routing packets.

Network mask — The portion of an IP address that identifies the network.

Node — Each computer, workstation, or device on a network.

Octet — A traditional term for each of the four 8-bit numbers that make up an IP address. For example, the IP address 206.96.103.114 has four octets.

Open Systems Interconnect (OSI) — A seven-layer (application, presentation, session, transport, network, data-link, physical) model of communications supported by a network. Refers to software and firmware only.

Packets — Network segments of data that also include header, destination addresses, and trailer information.

Physical layer — The OSI layer responsible for interfacing with the network media (cabling).

PPP (Point-to-Point Protocol) — A common way PCs with modems can connect to an internet. The Windows Dial-Up Networking utility, found under My Computer, uses PPP.

Presentation layer — The OSI layer that compresses and decompresses data and interfaces with the Application layer and the session layer.

Protocol — A set of preestablished rules for communication. Examples of protocols are modem parity settings and the way in which header and trailer information in a data packet is formatted.

Repeater — A device that amplifies weakened signals on a network.

Request for Comment (RFC) — A document presented to the technical community to propose and describe in detail a new standard to be adopted by the community at large. Search for and view RFCs at *www.rfc-editor.org*.

Reverse Address Resolution Protocol (RARP) — Translates the unique hardware NIC addresses into IP addresses (the reverse of ARP).

RJ-45 connector — A connector used on an Ethernet 10BaseT (twisted-pair cable) network. An RJ-45 port looks similar to a large phone jack.

Route discovery — When a router rebuilds its router tables on the basis of new information.

Router — A device or box that connects networks. A router transfers a packet to other networks only when the packet is addressed to a station outside its network. The router can make intelligent decisions as to which network is the best route to use to send data to a distant network and works at the Transport and Network layers of the OSI model.

Router table — Tables of network addresses that also include the best possible routes (regarding tick count and hop count) to these networks. *See* Tick count and Hop count.

Segmentation — To split a large network into smaller segments that are connected to each other by routers. This is done to prevent congestion as the number of nodes increases.

Session layer — The OSI layer that makes and manages a connection between two nodes of the network.

Signal-regenerating repeater — A repeater that "reads" the signal on a baseband network and then creates an exact duplicate of the signal, thus amplifying the signal without also amplifying unwanted noise that is mixed with the signal.

SLIP (Serial Line Internet Protocol) — An early version of line protocol designed for home users connecting to the Internet. SLIP lacks reliable error checking and has mostly been replaced by PPP.

SMTP (Simple Mail Transfer Protocol) — A common protocol used to send e-mail across a network.

Socket — A virtual connection from one computer to another such as that between a client and a server. Higher-level protocols such as HTTP use a socket to pass data between two computers. A socket is assigned a number for the current session, which is used by the high-level protocol.

Star topology — A network design in which nodes are connected at a centralized location.

Static IP addresses — IP addresses permanently assigned to a workstation. In Windows 9x, this can be done under Dial-Up Networking, Server Type, TCP/IP settings. Specify an IP address.

Subnet mask — Defines which portion of the host address within an IP address is being borrowed to define separate subnets within a network. A 1 in the mask indicates that the bit is part of the network address, and a 0 indicates that the bit is part of the host address. For example, the subnet mask 255.255.192.0, in binary, is 11111111.11111111.11000000.00000000. Therefore, the network address is the first two octets and the subnet address is the first two bits of the third octet. The rest of the IP address refers to the host.

Subnetworks or **subnets** — Divisions of a large network, consisting of smaller separate networks (to prevent congestion). Each subnetwork is assigned a logical network IP name.

Switch — A device that is used to break a large network into two smaller networks in order to reduce traffic congestion. A switch uses MAC addresses to determine which network to send a packet.

TCP/IP (Transmission Control Protocol/Internet Protocol) — The suite of protocols developed to support the Internet. TCP is responsible for error checking, and IP is responsible for routing.

Tick count — The time required for a packet to reach its destination. One tick equals 1/18 of a second.

Token — A small frame on a Token Ring network that constantly travels around the ring in only one direction. When a station seizes the token, it controls the channel until its message is sent.

Token ring — A network that is logically a ring, but stations are connected to a centralized multistation access unit (MAU) in a star formation. Network communication is controlled by a token.

Trailer — The part of a packet that follows the data and contains information used by some protocols for error checking.

Transceiver — The bidirectional (transmitter and receiver) component on a NIC that is responsible for signal conversion and monitors for data collision.

Transport layer — The OSI layer that verifies data and requests a resend when the data is corrupted.

URL (Uniform Resource Locator) — A unique address that identifies the domain name, path, or filename of a World Wide Web site. Microsoft's URL is: *http://www.microsoft.com/*

User Datagram Protocol (UDP) — A connectionless protocol that does not require a connection to send a packet and does not guarantee that the packet arrives at its destination. (A data packet was once called a datagram.)

Windows Internet Naming Service (WINS) — A Microsoft resolution service with a distributed database that tracks relationships between domain names and IP addresses. Compare to DNS.

Review Questions

1. What happens if an Ethernet network detects a transmission collision?
2. List and describe three types of cables that can be used on an Ethernet network.
3. What is the function of a router in a network environment? How is a router different from a bridge?
4. What type of connector is used on Ethernet Thinnet? On Ethernet 10BaseT?
5. What Windows 9x utility enables you to easily connect two PCs with a parallel or serial cable?
6. When computer A initates a connection to computer B, then computer A is called the _____ computer and computer B is called the _____ computer.
7. A device that belongs to more than one network and serves as the connection point between the two is called a _____.
8. In a star topology, the device that all computers connect to is called the _____.
9. The OSI layer responsible for error checking and guaranteeing successful delivery of data is the _____ layer.
10. A network card manages the _____ and _____ layers of the OSI model.
11. What is the reserved IP address that is used to refer to yourself?
12. List and briefly describe the seven network layers.
13. Describe a client/server network.
14. Use Windows Help, and describe how to use FTP to obtain a missing driver from the Microsoft web site.
15. List three of the largest ISPs.
16. Give an example of a Class C Internet address.
17. What organization is responsible for regulating the assignments of Internet addresses?
18. What are the advantages of dynamically assigned IP addresses?
19. List five main domain name extensions used in the United States.
20. What is the domain name extension for Harvard University? For Microsoft Corporation? For the White House?
21. What class does the IP address 130.200.50.3 belong in?
22. What is the subnet mask for Class C IP addresses on a network where 1 bit of the host address is used for the subnet address? How many subnets are possible using this arrangement?
23. Why would an organization use a WAN? What type of organization would use a WAN?
24. What utility is commonly used to "transfer" files on the Internet?
25. What is the purpose of Telnet?

PROJECTS

Practice Dial-Up Networking Skills with Windows 9x

1. Open My Computer and open the Dial-Up Networking folder.
2. Double-click the **Make New Connection** option.
3. Enter the name **TEST** for the name of the computer that you are dialing. Click **Next**.
4. Enter your home phone number. Click **Next**.
5. Click the **Finish** button to create the Test dial-up.
6. Double-click the newly created Test dial-up icon, and confirm that it dials out correctly. Describe what happens.

Use the PPPLog.txt File for Troubleshooting

Set Windows 9x so that the PPPLog.txt file is used to record events. Reboot the PC and make a good connection to the Internet, using a modem. Print the log file. This printout of a good connection can later be used to compare to a log file of a bad connection to help identify problems.

Now cause an error to occur in the dial-up connection to the Internet by setting a wrong configuration for TCP/IP (make a note of the correct configuration before you change it!). Attempt the connection. Print the log file for the bad connection and compare the two files. At what point during the connection did it fail? Restore the TCP/IP configuration to the correct value and verify that all is well.

Practice TCP/IP Networking Skills

While using TCP/IP on a network with or without Dial-Up Networking (such as while connected to the Internet), answer these questions:

1. What is your current IP address?
2. Disconnect and reconnect. Now what is your IP address?
3. Are you using dynamic or static IP addressing? How do you know?
4. What is your adapter address?
5. What is your default gateway IP address?
6. What response do you get when you PING the default gateway?

Using Windows 9x Help

Click the **Start** button and select **Help**. Search for "Internet," and write down a step-by-step set of directions that can be used to connect to the Internet using Dial-Up Networking.

Direct Cable Connection

Using either a null modem cable or a parallel cable, connect two computers using direct cable connection under Windows 9x. After the connection is made, use Explorer on the guest computer to copy a file from the host computer. Next, reverse roles, making the host the guest computer, and the guest the host computer. Copy a file from the host to the guest computer.

Dial-Up Networking

Work with a partner on this project. You each need a PC with Windows 9x or Windows NT, a modem, and a phone line. For two computers with Windows 95, one of the PCs must have Microsoft Plus! in order to be set up to receive incoming calls. Follow the directions in the chapter to connect the two computers using Dial-Up Networking over phone lines. After the connection is made, use Explorer to share files between the two computers.

Using a Null Modem Cable with Windows NT

A null modem cable can be used by Windows NT to communicate to another PC over a serial port. Install a null modem cable as though it were a modem. In the list of supported modems, select **Standard Modem Types** as the manufacturer, and select **Dial-Up Networking Serial Cable between 2 PCs** as the modem model.

Using two Windows NT PCs and a null modem cable, install and run Dial-Up Networking to establish communication between the PCs. Map a network drive from one PC to the other.

Building a Peer-to-Peer Network

Follow these directions to build a peer-to-peer network using network cards and a Microsoft network:

1. Obtain the following materials:
   - Two computers with Windows 9x
   - Network cards for each computer
   - Cabling and connectors for the network cards
2. Install the NICs. Check the configuration in Windows 9x against the card documentation.
3. Select the client software to be **Client for Microsoft Networks**.
4. Add the service **File and Printer Sharing**. Verify that File and Printer Sharing is running from the Network window.
5. Share a folder or folders on the hard drive. If you have a printer connected, share the printer.
6. Reboot both PCs and verify that you are connected, by browsing the Network Neighborhood of each PC.

Back Up Network Files

Look on a PC that is connected to a Novell NetWare LAN. Which entries in the AUTOEXEC.BAT file can you identify as commands used to load network software? Which directory contains the NetWare software? Print the contents of NET.CFG in this directory. What is the drive letter of the network drive used to log on to the LAN?